VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA NÁRODOHOSPODÁŘSKÁ

Bitcoin a jeho postavení na finančních trzích

Bitcoin and Its Position on Financial Markets

Student: Jiří Chudoba

Vedoucí bakalářské práce: Ing. Stanislav Kappel

Ostrava 2015

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra národohospodářská

Zadání bakalářské práce

Student: **Jiří Chudoba**

Studijní program: B6202 Hospodářská politika a správa

Studijní obor: 6202R027 Národní hospodářství

Téma: Bitcoin a jeho postavení na finančních trzích
Bitcoin and Its Position on Financial Markets

Zásady pro vypracování:

1. Úvod
2. Peníze – jejich pojetí, funkce a význam
3. Vznik a princip fungování Bitcoinu
4. Cena Bitcoinu na finančních trzích
5. Závěr

Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků bakalářské práce
Seznam příloh
Přílohy

Seznam doporučené odborné literatury:

CIAIAN, P., M. RAJČÁNIOVÁ and D. KANCS. The Economics of BitCoin Price Formation. In *EERI Research Paper Series*. 2014, No. 8, pp. 2-22. ISSN 2031-4892.
JÍLEK, Josef. *Peníze a měnová politika*. Praha: Grada Publishing, 2004. ISBN 80-247-0769-1.
REVENDA, Zbyněk. *Peníze a zlato*. 2. vyd. Praha: Management Press, 2013. ISBN 978-80-7261-260-4.

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Stanislav Kappel**

Datum zadání: 21.11.2014
Datum odevzdání: 07.05.2015

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA * OSTRAVA Ekonomická fakulta 1

doc. Ing. Zuzana Kučerová, Ph.D.
vedoucí katedry

prof. Dr. Ing. Dana Dluhošová
děkanka fakulty

Prohlašuji, že jsem celou práci, včetně všech příloh, vypracoval samostatně.

V Karviné dne 27.4.2015

Jiří Chudoba
.....
jméno a příjmení studenta

Poděkování

Tímto bych chtěl poděkovat panu Ing. Stanislavu Kappelovi za cenné rady, připomínky a pomoc při vypracování této bakalářské práce.

Obsah

1 Úvod

Rozvoj informačních technologií a obzvláště internetu v relativně nedávné době umožnil mimo jiné i rozšíření služeb jako internetové bankovnictví, nákupy z pohodlí domova apod. Tyto služby by však nemohly fungovat bez možností plateb na dálku. Ty skýtají některá úskalí, z nichž tím hlavním je nutnost účasti třetí strany. Ať už jde o bankovní převod, platbu platební kartou nebo prostřednictvím služby PayPal, žádný z těchto systému nedokáže v tomto ohledu napodobit klasickou platbu fyzickým oběživem. Může vůbec existovat platební systém, který by umožňoval rychlé provádění transakcí mezi nakupujícím a prodávajícím, aniž by byla nutná participace důvěryhodné třetí strany, a zároveň byly znemožněny podvody? Odpověď zní ano, Bitcoin tohle dokáže. A nejen to. Bitcoin není jen platební systém, ale i digitální měna, kterou je možné využít k nákupu zboží a služeb. V poslední době je Bitcoin relevantní i jako investiční aktivum, a dá se s ním také obchodovat na burzách.

Bitcoin vznikl v roce 2008, jde tedy o stále ještě relativně novou technologii. V České republice je Bitcoin málo rozšířený a relativně neznámý, neexistuje proto téměř žádná odborná literatura na toto téma v českém jazyce. Informace týkající se Bitcoinu potřebné pro zhotovení této práce byly získány z výhradně cizojazyčných zdrojů, především z vědeckých článků, dokumentů a internetových portálů a stránek psaných v anglickém jazyce. Kvůli absenci české terminologie pro danou problematiku jsou v textu v některých případech zachovány anglické výrazy. Kde bylo možné přeložit odborné termíny bez ztráty původního významu, byly v práci použity nejbližší české ekvivalenty.

Výběr tématu práce byl ovlivněn pozitivním vztahem autora k novým technologiím a internetu obecně. Pro autora práce proto bylo dané téma velmi atraktivní a pokládá jej za dostatečně aktuální. Důvodem pro zpracování práce na toto téma byla rovněž skutečnost, že Bitcoinem se příliš mnoho prací nezabývá, a ty práce které jej zkoumají, spíše popisují jeho technickou stránku nebo se snaží jen o zvýšení povědomí o této digitální měně. Tato práce nezachází do přílišných technických podrobností, ale je na Bitcoin zaměřena převážně z ekonomického hlediska.

Cílem této bakalářské práce je empiricky ověřit vliv finančních a makroekonomických ukazatelů na vývoj ceny Bitcoinu.

Naplnění tohoto cíle bude dosaženo použitím několika vědeckých metod. Na začátku bude provedena syntéza teoretických poznatků na základě rešerše literatury, dokumentů a

vědeckých článků na dané téma. Později v empirické části práce pak bude použita deskriptivní a korelační analýza.

Práce je rozdělena do tří částí, které jsou dále rozděleny na jednotlivé kapitoly a podkapitoly. Předmětem první části práce jsou peníze obecně. Je zde popsáno jaké podoby měly peníze v minulosti a jak probíhal jejich vývoj do podob, ve kterých existují dnes. Je zde také uvedeno, co se rozumí pod pojmem peníze z teoretického a empirického hlediska. Tato část dále obsahuje kapitoly, jejichž předmětem je definice funkcí peněz, resp. pojmu měna. Závěr a také největší díl této části je věnován kapitole o tvorbě a zániku peněz. Obsah této kapitoly je obzvláště důležitý pro pochopení základních principů, kterými se Bitcoin liší od standardních forem peněz.

V druhé části je již probírána problematika Bitcoinu a jsou zde popsány jeho elementární vlastnosti. Důležitým bodem této části je vysvětlení důvodů, proč nemůže být Bitcoin považován za virtuální měnu. Dále je zde také kapitola, jejímž předmětem je autor Bitcoinu, Satoshi Nakamoto a jeho záhadná identita. Poslední dvě kapitoly této části práce mají spíše techničtější charakter a popisují hlavní principy a mechanismy těžby Bitcoinů, resp. procesu uskutečňování transakcí.

Třetí část má převážně empirický charakter. Pomocí korelační analýzy jsou zde ověřovány vlivy vybraných finančních a makroekonomických ukazatelů na cenu Bitcoinu. Jsou zde také identifikovány hlavní faktory působící na vývoj ceny Bitcoinu na finančních trzích. Každá ze tří částí vždy na konci obsahuje stručné shrnutí hlavních myšlenek.

2 Peníze - jejich pojetí, funkce a význam

Než bude možné přejít k samotné problematice Bitcoinu, je třeba si uvědomit, že Bitcoin má být především měna. Tudíž jeho základní funkcí je sloužit jako platidlo. Pro rozhodnutí jestli Bitcoin má předpoklady stát se platidlem, tedy penězi, je nutné nejdříve pochopit, co je rozuměno pojmem peníze. V této kapitole bude nejdříve stručně popsán historický vývoj peněz a budou uvedeny definice peněz, jak z teoretického, tak z empirického hlediska. Dále budou vysvětleny funkce peněz a pojem měna. V neposlední řadě budou zodpovězeny otázky kde, kdy a jak dochází ke vzniku a zániku peněz. Tato část bude na konci uzavřena shrnutím obsahu probíraných kapitol.

2.1 Historický vývoj peněz

Počátky vzniku peněz je nutné hledat v dobách pravěkých kultur, kdy dochází k prvním známkám dělby práce. Člověk tehdy pochopil, že je lepší zaměřit se pouze na pracovní činnost, pro kterou je dostatečně fyzicky a psychicky vybaven, a kterou dokáže provádět nejefektivněji. Takovému jevu se říká specializace. Bez ní je práce méně produktivní, tzn. méně účinná. Jedinci, kteří se specializují, produkují jeden nebo několik málo různých statků v mnohem větším objemu, než sami pro sebe potřebují. Ostatní potřeby uspokojují směňováním svých přebytečných statků za statky jiných. Přestávají tak být izolovaní a stávají se závislými na ostatních osobách. Výměnu výsledků pracovních činností umožňuje mechanismus zvaný směna. Konkrétně při výměně zboží za zboží je to tzv. barter (Jurečka a kol., 2010).

Jak uvádí Jílek (2004), s rozšiřováním sortimentu zboží a služeb určených pro směnu se ukázalo, že barterová směna má některé velké nevýhody. Jednou z nich je skutečnost, že vyhledávání obchodního partnera k realizaci směny je časově náročné a vyžaduje značné úsilí, jinými slovy způsobuje vysoké transakční náklady. Příkladem je situace, kdy osoba A má zájem o zboží osoby B, ale ta za něj požaduje zboží osoby C. Černohorský a Teplý (2011) dodávají ještě nedělitelnost některých druhů zboží. Např. když osoba A má zájem o zboží osoby B, ale kvůli vyšší hodnotě svého zboží je osoba A nucena požadovat velké množství zboží osoby B nebo provést směnu v nevýhodném poměru.

Časem proto došlo k nahrazení barterové směny nepřímou směnou. Ze spotřeby se vyčlenily určité druhy zboží, které plnily funkci zprostředkovatele směny. Tak vznikly tzv. komoditní peníze. Revenda (2013) uvádí širokou škálu komodit, které se používaly jako ekvivalent pro transakce, od dobytku, obilí, soli a různých nástrojů používaných v době kolem

3500 let př. n. l až po mušle používané kolem roku 1200 př. n. l. v Africe a jihovýchodní Asii. Avšak ne každé zboží bylo k plnění funkce peněz stejně vhodné. Jako nejvhodnější se postupným vývojem ukázalo používání drahých kovů, které svými přírodními vlastnostmi vyhovují požadavkům obecně přijímaného platebního prostředku. Kovy jako zlato, stříbro, měď jsou homogenní (stejnorodé), snadno dělitelné a relativně odolné vůči opotřebení. Díky těmto atributům se staly perfektními kandidáty pro ražbu mincí, jejíž počátky se datují do 6. až 7. stol. p. n. l. (Revenda, 2013).

Mincovní systém operoval s oběhem plnohodnotných peněz, především zlatých a stříbrných mincí. To znamená, že kupní síla každé mince byla odvozena od váhového množství drahého kovu v ní obsažené a nákladů na její ražbu. S rozvojem obchodování a nárůstem množství transakcí ke konci středověku se pak objevily první formy bankovek. Jílek (2004) uvádí, že jako první bankovky se používaly zlatníky vydávané stvrzenky o množství a ryzosti uloženého drahého kovu. Tyto stvrzenky byly kryty drahými kovy v poměru 1:1. Zlatníci byli předchůdci bankéřů, kteří přijímali vklady a ty za účelem zisku dále půjčovali. Časem ale zjistili, že mohou poskytovat půjčky, aniž by předtím přijali odpovídající množství drahého kovu ve formě vkladů, což vedlo k emisi bankovek, jež nebyly kryty drahými kovy. Empirické zkušenosti zlatníků, resp. později bankéřů, prokázaly velmi nízkou pravděpodobnost, že si vkladatelé přijdou vyzvednout svůj drahý kov všichni najednou a tak banky vydávaly více poukázek na drahý kov, než kolik ho ve skutečnosti měly. To byl počátek neplnohodnotných peněz.

Tyto papírové peníze nejprve jen doplňovaly oběh zlatých a stříbrných mincí, později je však společně s neplnohodnotnými kovovými penězi zcela nahradily, neboť náklady na jejich oběh jsou výrazně nižší. Neplnohodnotné papírové a kovové peníze mají prakticky nulovou vnitřní hodnotu. Jurečka a kol. (2010, s. 45) dodává, že *„hodnota těchto peněz je založena na důvěře, že budou přijaty jako kupní a platební prostředek jinými subjekty společnosti.“* Jílek (2004) nazývá tento jev revolucí v peněžnictví. Množství peněz a růst peněžní zásoby již nebyly ničím omezeny, čímž se otevřely netušené možnosti pro nekontrolovanou úvěrovou emisi. Rostoucí množství nově emitovaných bankovek způsobovalo pokles jejich kupní síly a vedlo k nekontrolovatelné inflaci. Zanedbatelné nebyly ani příležitosti k bankovním podvodům. Je pochopitelné, že držitelé, jejichž bankovky byly, jak již bylo dříve uvedeno, směnkami na drahý kov, se obávali neschopnosti bank dodržet své závazky a v případě potřeby vyplatit zlato v poměru 1:1. Velký nápor požadavků na výměnu bankovek za drahý kov tak vedl ke krachu řady bank. Bylo zřejmé, že tato situace se neobejde

bez regulačních omezení daných nějakou centrální autoritou. Řešením se ukázal vznik centrálních bank a provádění novodobé měnové politiky.

Neplnohodnotné peníze později získaly podobu zápisů na účtech představujících závazky bank vůči klientům. Peníze v této formě se nazývají účetní nebo také bezhotovostní peníze a jsou důležitým prvkem v procesu tvorby a zániku peněz, o němž se pojednává v kapitole 2.5.

2.2 Definice peněz

Jak píše Revenda (2013), definice peněz lze rozdělit na teoretické a empirické, kde teoretické definice se zaměřují na podstatu peněz a empirické definice vycházejí z vymezení množství peněz v oběhu.

Jílek (2004) i Revenda (2013) se shodují, že z teoretického hlediska se za peníze považuje vše, co je všeobecně přijímáno při placení za zboží a služby nebo při úhradě dluhu. Revenda (2013) zdůrazňuje aspekt všeobecnosti a s ním úzce související důvěryhodnost peněz, jež je obzvláště důležitá u papírových peněz s minimální vnitřní hodnotou. Důvěryhodnost papírových peněz může být podpořena možností směny za drahý kov nebo zákonným ustanovením, které určuje, že právě takovými penězi lze platit na území daného státu. U bezhotovostních peněz, jež mají podobu zápisů na účtech v bankách, hraje důležitou roli důvěryhodnost těchto bank, neboť právě do nich zpravidla ukládají subjekty své vklady.

Jak uvádí Revenda (2013), empiricky jsou peníze definovány peněžními neboli měnovými agregáty, jež jsou sestavovány centrálními bankami. Pomocí měnových agregátů může centrální banka sledovat a regulovat vývoj množství peněz v oběhu a předpovídat vývoj jiných makroekonomických veličin, jako je cenová hladina či agregátní výstup (především hrubý domácí produkt). Peněžní agregáty bývají označovány písmenem M a číslicí zpravidla od 1 do 3 podle stupně likvidity. Likvidita udává jak rychle a s jakými náklady lze převést daný peněžní agregát na bezprostřední platební prostředky. Nejlikvidnější jsou prostředky v peněžním agregátu M1, neboť obsahuje hotovostní oběživo (tj. bankovky a mince) a vklady na běžných účtech. Dále platí, že každý další peněžní agregát obsahuje všechna aktiva obsažená v předchozím agregátu společně s jinou méně likvidní složkou. Měnový agregát, který je pro centrální banku a pro provádění její měnové politiky reprezentativní nese název peněžní zásoba.

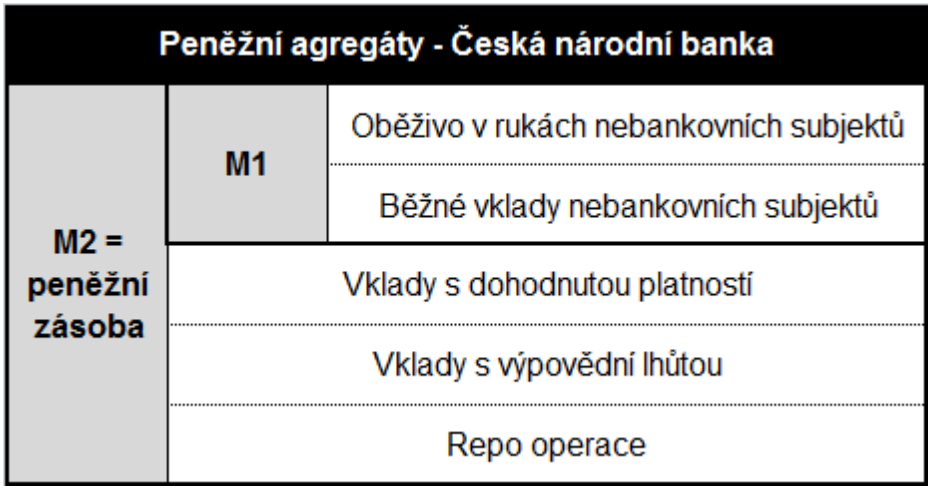
Jílek (2004) vyčleňuje z agregátu M1 veškeré oběživo emitované centrální bankou držené rezidenty i nerezidenty a uvádí jej jako peněžní agregát M0. Peněžní agregát M1

označuje stejně jako Revenda (2013) termínem úzké peníze, agregáty M2 a M3 nazývá širšími penězi. Revenda (2013) ještě navíc rozlišuje pojem střední peníze pro agregát M2 a široké peníze pro M3.

Jílek (2004) dodává, že kromě oběživa jsou do peněžních agregátů zahrnuta pouze aktiva držená rezidenty. Za rezidenty jsou považovány tuzemské právnické a fyzické osoby a dále pak pobočky zahraničních bank a zahraniční vlastníci budov a pozemků, jež mají střed ekonomického zájmu na ekonomickém území České republiky. Pro zahraniční právnické a fyzické osoby toto platí, pokud ekonomicky působí na území České republiky alespoň jeden rok. Nerezidenti jsou fyzické a právnické osoby, které nesplňují kritéria pro rezidenty. Definice jednotlivých peněžních agregátů se mohou v různých zemích lišit a někdy dochází v rámci jedné země také ke změnám v čase.

Česká národní banka (2014) uvádí, že likvidní aktiva rezidentů České republiky v cizích měnách mohou být velmi blízkými substituty aktivům v českých korunách. Proto peněžní agregáty zahrnují tato aktiva, pokud jsou uložena u měnových finančních institucí nacházejících se v České republice. Schéma peněžních agregátů podle České národní banky a Evropské unie, jak je uvádí Revenda (2013), je znázorněno na obrázku 2.1 a 2.2.

Obr. 2.1 Peněžní agregáty podle ČNB



Zdroj: Revenda (2013), vlastní zpracování

Obr. 2.2 Peněžní agregáty harmonizované podle EU

<table>
<tr><th colspan="4">Peněžní agregáty - harmonizace podle EU</th></tr>
<tr><td rowspan="6">M3 ("široké peníze")</td><td rowspan="4">M2 ("střední peníze")</td><td rowspan="2">M1 ("úzké peníze")</td><td>Oběživo v rukách nebankovních subjektů</td></tr>
<tr><td>Běžné vklady nebankovních subjektů</td></tr>
<tr><td colspan="2">Vklady s dohodnutou platností do 2 let</td></tr>
<tr><td colspan="2">Vklady s výpovědní lhůtou do 3 měsíců</td></tr>
<tr><td colspan="3">Repo operace</td></tr>
<tr><td colspan="3">Akcie a podílové listy fondů peněžního trhu</td></tr>
<tr><td colspan="3">Emitované dluhové cenné papíry do 2 let</td></tr>
</table>

Zdroj: Revenda (2013), vlastní zpracování

Zvláštní pozornost zaslouží také schéma peněžních agregátů podle amerického Federálního systému rezerv (dále jen „Fed“) v podobě, kterou uvádí Mishkin (2004). Fed je centrální bankovní autoritou ve Spojených státech a je zodpovědný za provádění monetární politiky. Na základě mnohých studií a v důsledku historického vývoje rozlišuje Fed agregáty M1, M2 a M3. Do nejlikvidnějšího agregátu M1 je zahrnuto oběživo společně s vklady na běžných účtech obchodních bank i spořících institucí a cestovní šeky. Zvláštní součástí tohoto agregátu jsou šekovatelné vklady, např. tzv. účty NOW (Negotiable Order of Withdrawal), které při splnění určitých podmínek kombinují výhody běžných účtů a termínovaných vkladů. Do agregátu M2 patří M1 plus spořící vklady, účty vkladů peněžního trhu, podílové listy fondů peněžního trhu (nevlastněné institucionálními investory) a malé[1] termínové vklady a dohody o zpětném odkupu. Agregát M3 přidává k M2 velké termínové vklady a dohody o zpětném odkupu společně s podílovými listy fondů peněžního trhu (vlastněné institucionálními investory) a eurodolary.

Teď je již jasné, jaký typ aktiv obsahují jednotlivé peněžní agregáty. Nabízí se otázka, do kterého agregátu by se dal zařadit Bitcoin. Nicméně odpověď není tak úplně snadná. Za předpokladu, že všechny subjekty v ekonomice přijímají Bitcoin jako formu platby za zboží a služby, lze Bitcoin zařadit mezi nejlikvidnější aktiva s podobnými vlastnostmi jako vklady na běžných účtech, avšak s nižšími nebo žádnými náklady. Ve

[1] „Malé“ v tomto případě znamená „o částkách nižších než 100 000 USD“ (Jílek, 2004).

skutečném světě však tento předpoklad v současné době neplatí, proto je v některých případech nutné nejdříve převést bitcoiny na „konvenční“ platební prostředky. Nejčastěji se tak děje prostřednictvím prodeje na virtuální burze. Podobné vlastnosti mají např. krátkodobé cenné papíry, jež jsou ale rozhodně méně likvidní než aktiva v prvním případě.

2.3 Funkce peněz

Jílek (2004), Mishkin (2004) i Revenda (2013) uvádějí 3 funkce, které mají peníze v ekonomice. Peníze plní funkci prostředku směny, účetní jednotky a uchovatele hodnoty. Riegel (2007) přidává ještě čtvrtou, funkci měřítka a prostředku úhrady odložených plateb.

Ve funkci prostředku směny se peníze uplatňují při placení za zboží a služby a při úhradě dluhu. Historicky tato funkce umožnila nahrazení barterové, tj. přímé směny, směnou nepřímou. Peníze díky této funkci výrazně snížily transakční náklady, vznikající při snaze nalézt obchodního partnera pro uskutečnění přímé směny (Revenda 2013).

Díky funkci účetní jednotky je možné stanovit cenu veškerého zboží, služeb, práce, kapitálu, cizích měn apod. Tato funkce rovněž umožňuje vedení účetních záznamů a také zjednodušuje směnu. Bez ní by směna zboží a služeb probíhala velmi obtížně, neboť cena každého statku by musela být vyjádřena v počtech ostatních statků. Např. cena jednoho banánu = 2 jablka = 4 jahody = 16 borůvek atd. Při širokém sortimentu zboží se jeví taková představa jako téměř nemožná. Navíc u některých druhů zboží by směna nemohla proběhnout z důvodu jejich nedělitelnosti. Např. 1 stůl = 2,5 židle (Revenda 2013).

Jsou-li peníze dočasně staženy z oběhu, např. ve formě úspor, je důležité, aby měly funkci uchovatele hodnoty. To znamená, aby bylo ekonomickým subjektům umožněno si peníze uložit a použít je v až budoucnu, neboli překonat časový nesoulad mezi příjmy a výdaji. Jinými slovy je důležité, aby si peníze zachovaly svoji kupní sílu v čase. Kupní síla peněz vyjadřuje množství zboží a služeb, které lze v různém čase při daných cenách za peníze získat. Kupní síla peněz se odvíjí od vývoje cenové hladiny. Její růst způsobí pokles kupní síly peněz a naopak. Očekávají-li subjekty zvýšení cen zboží a služeb, bude jejich motivace k držbě peněz nízká (Revenda 2013).

2.4 Měna

Černohorský a Teplý (2011) definují pojem měna jako národní formu peněz. V případě měny jako je euro, které se používá v členských zemích Evropské měnové unie, jde o nadnárodní formu peněz. Pojem měna je podmnožinou pojmu peníze, tj. za peníze jsou

považovány různé měny, avšak opačně tento vztah neplatí. Měnou na daném území, např. území České republiky, je pouze česká koruna. Každou měnu charakterizují její technické a ekonomické znaky. Mezi technické znaky měny patří název měny, hotovostní druhy, nominální struktura, dělení a kumulace, výlučnost měny a způsob stanovení měnového kurzu.

Je zřejmé, že každá měna musí mít svůj celý název, např. česká koruna, americký dolar, japonský jen atd. V mezinárodním pojetí se pro názvy měn používají třímístné písemné zkratky vycházející z mezinárodního standardu ISO 4217, vydávaného Mezinárodní organizací pro normalizaci (International Organization for Standardization), např. CZK, USD, JPY atd.

Hotovostní druhy představují bankovky a mince. Tento znak je společný pro většinu měn. Nominální struktura znamená dělení základní jednotky měny na menší jednotky a zároveň používání násobků základní nominální hodnoty. V případě české koruny to v současnosti znamená rozlišování mincí o nominálních hodnotách 1 Kč, 2 Kč, 5 Kč, 10 Kč, 20 Kč a 50 Kč a bankovek v hodnotách 100 Kč, 200 Kč, 500 Kč, 1000 Kč, 2000 Kč a 5000 Kč. Dělení a kumulace základní měnové jednotky v případě české koruny představuje dělení na 100 haléřů a kumulaci na desítky, sta, tisíce atd.

Výlučnost měny znamená, že přijímání určité měny ekonomickými subjekty na vymezeném území je vynuceno zákonným ustanovením. V České republice zákon č. 6/1993 Sb., o České národní bance ve znění pozdějších předpisů, udává, že peněžní jednotkou v České republice je koruna česká. Černohorský a Teplý (2011) dále uvádějí, že způsob stanovení měnového kurzu představuje různé možnosti stanovení hodnoty měny vůči ostatním měnám. V České republice stanovuje kurzy devizového trhu Česká národní banka na základě monitorování vývoje měn na mezibankovním devizovém trhu.

Ekonomickými znaky měny jsou charakter emise peněz a způsob zajištění měnové stability. Charakter emise peněz znamená způsob uvolňování peněz do oběhu a jejich stahování. Měnovou stabilitu v České republice zajišťuje Česká národní banka prováděním měnové politiky (Černohorský a Teplý, 2011).

2.5 Tvorba a zánik peněz

Pro účely pozdějšího porovnání v jedné z následujících kapitol je relevantní uvést principy tvorby a zániku „konvenčních“ peněz.

Jílek (2004) vysvětluje tvorbu a zánik peněz, neboli emisi a stahování peněz, pomocí postkeynesiánské teorie endogenních peněz. Ta spočívá v tom, že na rozdíl od neoklasické

kvantitativní teorie peněz nejsou obchodní banky považovány pouze za finanční zprostředkovatele, ale přímo za tvůrce peněz. Peníze v nich vznikají i zanikají a děje se tak především prostřednictvím poskytování, resp. splácení úvěru. Nutnou podmínkou je existence dlužníka. Centrální banka plní pouze roli věřitele poslední instance a její hlavní odpovědností je zajistit solventnost finančního sektoru (tj. zabránit vzniku deflačních tlaků spojených s neschopností splácet dluhy). Revenda (2013) přisuzuje centrální bance v procesu tvorby peněz o něco významnější roli, a to prostřednictvím emise peněz v podobě rezerv bank. V každém případě jsou peníze tvořeny pouze ve formě účetních peněz a až potom je možné vyměnit je za oběživo. Z tohoto hlediska je oběživo teoreticky nepotřebné. Procesy, jimiž vznikají účetní peníze, tak jak je uvádí Jílek (2004), jsou:

- poskytování úvěrů bankami nebankovním jednotkám,
- úročení vkladů a jiných závazků bank vůči nebankovním jednotkám,
- koupě majetku a služeb bankami od nebankovních jednotek (koupě hmotného i nehmotného majetku, dluhových i kapitálových cenných papírů, zlata apod.),
- výplat platů a odměn zaměstnancům a statutárním orgánům bank a
- výplatou dividend a tantiém (podílů členů představenstva a členů dozorčí rady na zisku).

Během těchto činností vznikají peníze v okamžiku, kdy jsou připsány na účet klienta, a zanikají při odepsání peněz z účtu klienta při provádění opačných operací (např. splácení úvěru). V zásadě platí, že k tvorbě peněz dochází, pokud banka při připsání peněz na účet klienta nestrhne stejný obnos z účtu jiného klienta, nebo neodečte-li jiná banka stejnou částku z účtu jiného klienta. Peníze tedy nevznikají prostřednictvím převodů peněz z účtu jednoho klienta na účet jiného klienta. Obdobně Jílek (2004) popisuje situaci obchodní banka – obchodní banka. Peníze nevznikají, pokud jedna banka poskytuje úvěr jiné bance, kupuje od ní majetek a služby nebo vyplácí dividendy jiné bance. Stejně tak peníze nezanikají, když banka splácí úvěr jiné bance, prodává majetek a služby jiné bance apod. Vznik a zánik peněz je proto podmíněn vztahem obchodní banka – klient (popř. zaměstnanec nebo člen statutárního orgánu banky), na němž jsou uvedené operace založeny. Peníze tak mohou být definovány jako některé závazky obchodních bank vůči klientům (nebo zaměstnancům a členům statutárních orgánů). Závazky vůči jiným obchodním bankám či centrální bance nejsou penězi, nazývají se likvidita. Závazky centrální banky vůči klientům, státu a obchodním bankám nepatří do peněžních agregátů, nespadají proto do definice peněz. Za

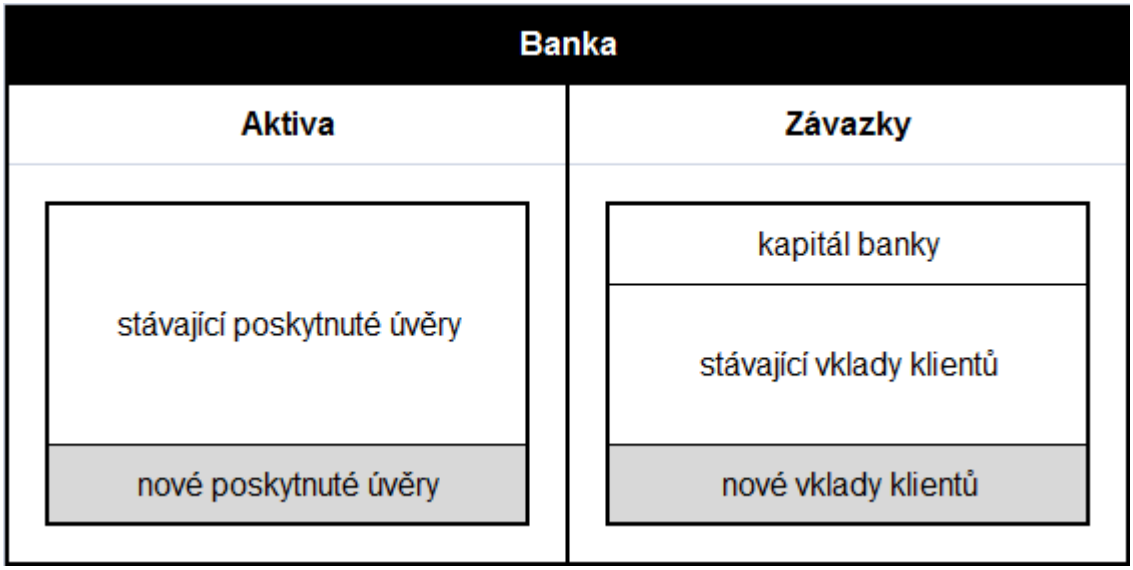
peníze je považováno pouze centrální bankou emitované oběživo s výjimkou oběživa na pokladnách bank, na pokladnách poboček zahraničních bank a na pokladnách centrální banky.

Revenda (2013) i Jílek (2004) tvrdí, že nejvíce peněz v bankovním systému vzniká prostřednictvím bezhotovostních úvěrů poskytovaných obchodními bankami nebankovním subjektům, tj. hlavně podnikům a domácnostem. Nejvíce peněz zaniká opačným způsobem, tj. splácením úvěrů včetně úroků nebankovními subjekty bankám. Zároveň platí, že tyto peníze nemusí vznikat a zanikat pouze v domácí měně, nýbrž také v měně jakékoliv jiné země.

Jílek (2004) uvádí, že i nebankovní jednotky mohou poskytovat úvěry, úročit vklady, nakupovat majetek a služby, vyplácet platy a odměny zaměstnancům a statutárním orgánům a vyplácet dividendy nebankovním akcionářům, avšak pouze do výše zůstatků na svých bankovních účtech, čímž se výrazně liší od obchodních bank. Obchodní banky jsou v tomto ohledu v podstatě neomezeny, jelikož na rozdíl od nebankovních jednotek není nutné, aby před poskytnutím úvěru, koupí majetku a služeb, výplatou platů a odměn zaměstnancům apod. nejdříve do banky někdo peníze přinesl. Obchodní bankám v tvorbě peněz nebrání absence vkladů. Teorie endogenních peněz totiž předpokládá, že úvěry vytvářejí vklady a ne naopak. Až když banka připíše peníze na účet klienta, může s nimi daný klient disponovat.

V následujícím textu bude tvorba a zánik peněz vysvětlena především na poskytování úvěrů obchodními bankami klientům, neboť jak již bylo výše uvedeno, jde o způsob, kterým v ekonomice vzniká a zaniká největší objem peněz.

Obr. 2.3 Tvorba peněz poskytováním nových úvěrů



Zdroj: Jílek (2004), vlastní zpracování

Jak píše Jílek (2004), poskytování úvěrů představuje pro účetnictví banky přírůstek na straně aktiv i na straně závazků (viz obr. 2.3). Při každém poskytnutém úvěru dochází k vytvoření pohledávky za klientem na straně aktiv a vytvoření závazku banky vůči klientovi na straně pasiv. Stejně tak dochází k nárůstu na obou stranách v účetnictví klientů, jimž banka úvěry poskytuje. Jak již bylo zmíněno výše, teoreticky bankám nebrání nic v tom, aby poskytovaly úvěry donekonečna. Chtějí-li ovšem banky maximalizovat zisk (jako každý racionálně uvažující ekonomický subjekt), musejí postupovat obezřetně. Do hry totiž vstupuje úvěrové riziko, tj. riziko, že poskytnutý úvěr dlužník nesplatí. Na základě úvěrového rizika banky hodnotí klienty a vybírají si pouze ty s nejlepším úvěrovým hodnocením. Existuje několik úrovní úvěrového hodnocení, obyčejně značené písmeny A, B a C, kde počet písmen (1 až 3) vyjadřuje rozdíly na jednotlivých úrovních, např. u subjektů s hodnocením AAA je nižší úvěrové riziko než u těch s hodnocením A, jsou ale pořád méně rizikové než BBB. Nejhorší hodnocení (označované D) obdrží subjekty, u nichž se riziko nesplacení úvěru blíží 100 %. Stanovení hranice pro poskytnutí úvěru, např. mezi úrovněmi B a CCC, záleží na averzi bank k riziku. Je-li banka více averzní vůči riziku, přestane poskytovat úvěry třeba na úrovni BB. Jiná banka může mít nižší averzi k riziku a tak poskytuje úvěry až do úrovně CC. *„Je uměním každé banky správně posoudit riziko každého klienta a rozhodnout o poskytnutí úvěru“* (Jílek, 2004, s. 48). Je obvyklé, že vývoj poskytování úvěrů víceméně kopíruje ekonomický cyklus. Obecně platí, že v dobách konjunktury jsou banky při poskytování úvěrů optimističtější a jejich averze k riziku klesá. Naopak v období krize rostou bankám náklady z důvodu nesplacených úvěrů, jež byly lehkomyslně poskytnuty v předchozích obdobích, a proto poskytují méně úvěrů. Jako příklad zde může posloužit finanční krize, která začala koncem roku 2008 ve Spojených státech, a která později přerostla v globální ekonomickou krizi.

Jílek (2004) zmiňuje ještě jeden aspekt výše uvedeného způsobu tvorby peněz. V souvislosti s tím, že obchodní banky pro tvorbu peněz nepotřebují žádné zdroje, ale naopak je při poskytování úvěrů samy tvoří, nelze přehlížet fakt, že je tento princip velmi příhodný pro zneužívání. V případě, že osoby ve vedení bank nejsou dostatečně kontrolovány bankovním dohledem, hrozí, že vedení banky nebo bankovní pracovníci, jež mají schvalování úvěrů na starosti, se začnou tímto způsobem obohacovat ve vlastní prospěch. Za úplatek a předem dohodnutou provizi zařídí bankovní pracovník schválení úvěru, u něhož je předem jasné, že nebude splacen. Jedná-li se o člena představenstva, může svými pravomocemi zařídit, že úvěr vůbec nebude procházet schvalovacím procesem a bude rovnou poskytnut. Banka časem začne na úvěr tvořit opravné položky a tím jej přesune z aktiv do nákladů.

Dočasný nedostatek likvidity může banka vyřešit půjčkou na mezibankovním trhu. Tvoří-li takovéto podvodné úvěry velkou část bankovních aktiv, hrozí situace, kdy bance přestanou ostatní banky půjčovat a zůstane odkázána pouze na své vkladatele. Bance nezbývá než zvýšit úrokové míry z vkladů, aby si udržela stávající a přilákala nové vkladatele. Jinak může dojít na tzv. „run“ na banku, tj. situace, kdy vkladatelé začnou hromadně vybírat své vklady, protože ztratili důvěru v banku. To obyčejně vede k bankrotu banky a za předpokladu, že takových bank existuje víc, i k finanční krizi. Některé banky jsou příliš velké na selhání, proto jim stát poskytne záchranu z prostředků státního rozpočtu. Tím může dojít k dluhové krizi. Obecně lze říct, že na bankrot banky doplatí vkladatelé nebo daňoví poplatníci.

Pro výše popsané nekalé praktiky se ujal pojem „tunelování“. Jde o světově rozšířený pojem, který původně vznikl v České republice a na Slovensku souvislosti s obřími tunely v 90. letech. Tunelování znamená podvodné zcizování majetku podniku většinovými vlastníky, někdy i osobami ve vedení podniků. Tunelovat lze banky i nebankovní podniky (Jílek, 2013).

2.6 Dílčí shrnutí

Na začátku této části byl stručně popsán historický vývoj peněz. Počátky peněz je možné nalézt v souvislosti s rozšířením směny, jež byla důsledkem rozvoje dělby práce a specializace. Prvním typem směny byl tzv. barter, tj. směna zboží za zboží. Časem se ukázalo, že barterová směna má některé velké nevýhody, proto byla nahrazena směnou nepřímou. Ze spotřeby se vyčlenily určité druhy zboží, které pak byly používány jako komoditní peníze. Nejvhodnějšími kandidáty se díky svým vlastnostem staly drahé kovy. Začaly se z nich razit plnohodnotné peníze – mince, jejichž kupní síla odpovídala váhovému množství drahého kovu v nich obsaženém a nákladů na jejich ražbu. Stvrzenky o množství drahého kovu uloženého u zlatníka (a později v bance) později sloužily jako první bankovky. To byl počátek neplnohodnotných peněz.

Následovala kapitola o definicích peněz. Teoreticky jsou peníze definovány jako vše, co je všeobecně přijímáno při placení zboží a služby nebo při úhradě dluhu. Empiricky jsou peníze definovány pomocí peněžních agregátů, které jsou sestavovány centrálními bankami. Jako příklady byla uvedena schémata peněžních agregátů podle ČNB, EU a Fedu.

V další kapitole byly vysvětleny funkce peněz. Těmi jsou zpravidla funkce prostředku směny, funkce účetní jednotky a funkce uchovatele hodnoty.

Následující kapitola obsahovala definici pojmu měna. Jde o národní, resp. nadnárodní formu peněz (v případě měn jako je Euro). Každou měnu charakterizují její technické a ekonomické znaky. Mezi technické znaky měny patří název měny, hotovostní druhy, nominální struktura, dělení a kumulace, výlučnost měny a způsob stanovení měnového kurzu. Ekonomickými znaky měny jsou charakter emise peněz a způsob zajištění měnové stability.

V závěrečné kapitole byly poskytnuty odpovědi na otázky kde, jak a kdy vznikají a zanikají peníze. Bylo tak učiněno pomocí postkeynesiánské teorie endogenních peněz. Nejvíce peněz v bankovním systému vzniká, když obchodní banky poskytují úvěry nebankovním jednotkám. Nejvíce peněz zaniká opačným způsobem, tj. splácením úvěrů včetně úroků nebankovními jednotkami bankám. Banky jsou při poskytování úvěrů teoreticky neomezeny, neboť není nutné, aby předtím někdo peníze do banky přinesl. Podle teorie endogenních peněz totiž úvěry vytvářejí vklady. Neznamená to však, že by banky poskytly úvěr každému, kdo o něj požádá. Banky své klienty hodnotí a vybírají si pouze ty s nejnižším rizikem nesplacení úvěru. Dochází-li k poskytování podvodných úvěrů, hovoří se o tzv. tunelování. Tvoří-li tyto úvěry velkou část aktiv, může se banka dostat do špatné finanční situace, popřípadě zbankrotovat. Zbankrotuje-li více bank najednou, může dojít k finanční krizi.

3 Vznik a princip fungování Bitcoinu

Trvalo několik tisíc let, než peníze dostaly podobu, v jaké je známe dnes. Zatím posledním evolučním stupněm peněz jsou v současnosti peníze elektronické neboli digitální, a s nimi spojený nástup digitálních měn. Bitcoin je specifickým typem digitální měny, jak bude podrobněji vysvětleno v kapitole 3.1. Ta je dále rozdělena na 4 krátké podkapitoly, které definují Bitcoin ze dvou různých hledisek, resp. vysvětlují odlišnosti od virtuálních měn a hlavní charakteristické znaky Bitcoinu. Předmětem druhé kapitoly je bližší pohled na záhadnou identitu autora Bitcoinu, Satoshiho Nakamota a na jeho roli v počátcích Bitcoinu. Následující dvě kapitoly mají spíše techničtější charakter a jsou zaměřeny na vysvětlení principů procesu těžby bitcoinů, resp. fungování transakcí. Obdobně jako v případě první části této práce je i tato část zakončena kapitolou dílčí shrnutí.

Hned v úvodu této části práce je důležité vyjasnit několik terminologických záležitostí doprovázející danou problematiku. Ačkoliv některé prameny[2] usilují o užívání jednotného pojmu „bitcoin“ ve všech případech, v této práci bude rozlišováno mezi pojmy „Bitcoin“ a „bitcoin“, aby nedocházelo k omylům, záměnám a nedorozuměním. Pojmem „Bitcoin“ bude označen online platební systém, založený na principu peer-to-peer sítě[3] a navržený v roce 2008, jehož autorem je Satoshi Nakamoto, a rovněž decentralizovaná digitální měna používaná v tomto systému. Pro účetní jednotku Bitcoinu bude použit pojem „bitcoin“.

Tato část práce čerpá v drtivé většině z cizojazyčných zdrojů, proto občas dochází k problémům s překladem, neboť daná problematika nemá přímý český ekvivalent.

3.1 Co je to Bitcoin?

Jak již bylo zmíněno v úvodu této části práce, Bitcoin je nutné chápat jako online platební systém založený na principu peer-to-peer sítě a rovněž jako decentralizovanou digitální měnu používanou v tomto systému. Nejprve bude vysvětlen Bitcoin ve smyslu digitální měny, neboť často dochází k záměně termínů „virtuální“ a „digitální“. Ač se na první pohled může zdát, že jde o označení pro jednu a tu samou vlastnost, není tomu tak.

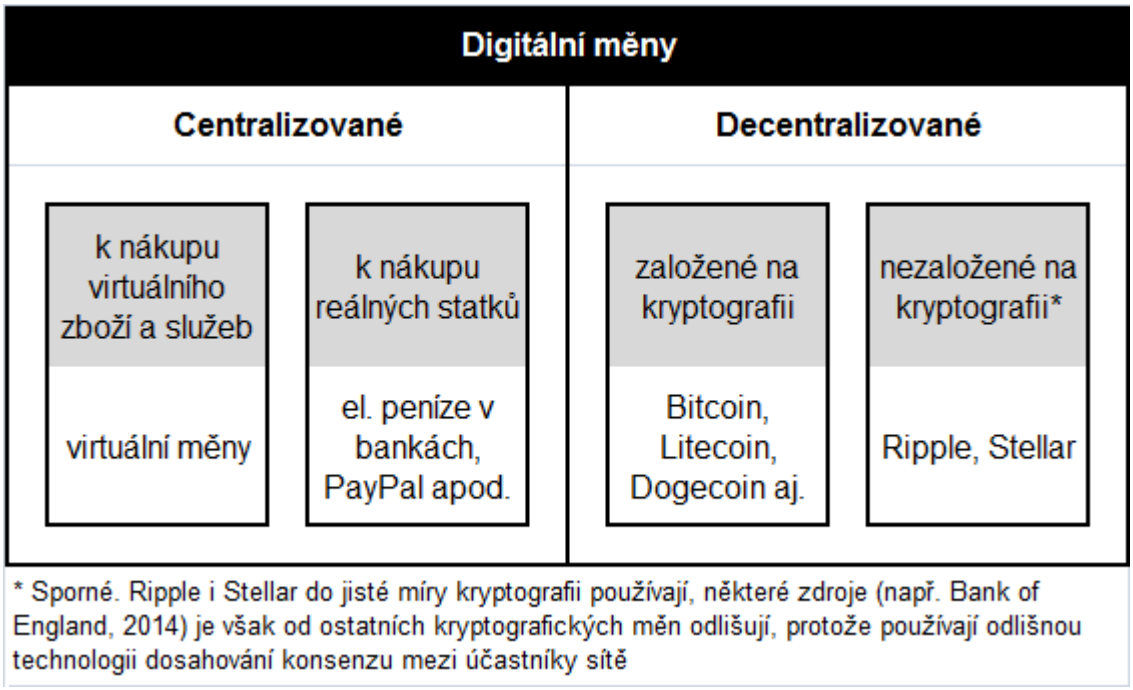
[2] Např. Vigna a Casey (2014) nebo Metcalf (2014).

[3] Peer-to-peer (zkráceně „P2P“) síť je typ počítačové sítě, v níž každý uzel (počítač) plní funkci klienta i serveru, přičemž všechny uzly jsou si rovny (Janssen, 2015a).

3.1.1 Bitcoin jako digitální měna

Wagner (2014) i Evropská centrální banka (2012) uvádí, že virtuální měna je typem digitální měny, ale opačně tento vztah neplatí. Wagner (2014) pak dále podotýká, že Bitcoin je taktéž typem digitální měny, avšak jiným a zásadně odlišným od virtuálních měn. Bitcoin je tzv. „kryptoměna[4]“, jež se dá jednoduše charakterizovat jako digitální měna používající kryptografii (neboli šifrování) k zabezpečování transakcí a k řízení emise nových jednotek.

Obr. 3.1 Schéma různých typů digitálních měn



Zdroj: ECB (2012), vlastní zpracování

Co je tedy digitální měna? Digitální měna, občas označovaná jako elektronické peníze, představuje peníze uchovávané a převáděné elektronicky. Do této definice tak spadají i účetní záznamy o prostředcích uložených na bankovních účtech uchovávané v elektronické podobě. Z toho vyplývá, že digitální měny existovaly již před vznikem Bitcoinu, z historie je možné uvést například E-gold[5] nebo Liberty Reserve[6]. Příčinou konce těchto digitálních měn byla podezření z praní špinavých peněz a následné zrušení vládou Spojených států. Ze

[4] Pro angl. termín „cryptocurrency“ neexistuje oficiální český ekvivalent, avšak pojem „kryptoměna“ se přímo vybízí. Alternativně pak připadá v úvahu ještě pojem „kryptografická měna“.

[5] E-gold byla digitální měna plně krytá zlatem a jinými drahými kovy, založená v roce 1996. Systém E-gold umožňoval uživatelům založit si účet, pořídit si na něj za reálné peníze určité množství zlata, a to pak používat jako digitální měnu (Wagner, 2014).

[6] Liberty Reserve byla digitální měna založená v roce 2006. Služba umožňovala uživatelům převést své dolary či eura na Liberty Reserve Dolary (resp. Liberty Reserve Eura) a směňovat je volně mezi sebou za relativně nízký poplatek (Wagner, 2014).

současnosti lze zmínit například široce rozšířený systém PayPal, který staví na již existující infrastruktuře bankovních účtů a kreditních (resp. debetních) karet. Společným znakem těchto digitálních měn a jejich hlavní odlišností od Bitcoinu je právě centralizace. Pro lepší ilustraci je na obr. 3.1 znázorněno schéma různých typů digitálních měn.

3.1.2 Virtuální měny

Proč tedy Bitcoin není virtuální měnou a v čem spočívá jejich hlavní odlišnost? Evropská centrální banka (2012) definuje virtuální měnu jako typ neregulované digitální měny, jejíž emise a kontrola nad ní je v rukou jejích tvůrců, a která je používána a všeobecně přijímána členy určité virtuální komunity. Tato definice bude nyní podrobněji vysvětlena.

S masivním rozvojem informačních technologií a obzvláště internetu v posledních přibližně dvaceti letech souvisí také vznik a rychlý nárůst počtu virtuálních komunit. Virtuální komunita je podle definice Evropské centrální banky (2012) místo v kyberprostoru, na kterém dochází k interakci jedinců za účelem sledování společných zájmů a plnění společných cílů. Pravděpodobně nejpopulárnějším příkladem virtuálních komunit jsou komunity internetových sociálních sítí jako je Facebook nebo Twitter. Existují však i komunity vytvořené pro jiné účely, např. sdílení videí (YouTube), sdílení znalostí a vědomostí (Wikipedia), život ve virtuální realitě (Second Life) nebo online zábavu (Steam) a spousty dalších. Charakteristikou některých virtuálních komunit je právě používání virtuální měny jako prostředku k placení za zboží a služby, jež tyto komunity nabízejí. V takových komunitách pak virtuální měna plní funkce prostředku směny a účetní jednotky tak, jako je plní peníze v reálné ekonomice[7]. Sporná zůstává pouze funkce uchovatele hodnoty z důvodu absence regulace. Wagner (2014) dokonce uvádí, že virtuální měny jsou primárně používány ke zprostředkování online zábavy ve virtuálních světech. Pojem „virtuální“ definuje jako „neexistující ve skutečném světě“, virtuální měny tudíž nejsou určeny k použití ve skutečném světě nebo k nákupu skutečných aktiv.

Společným znakem prakticky všech virtuálních měn je centralizace, neboť veškerá moc nad peněžní nabídkou těchto měn leží v rukou tvůrců a vývojářů virtuálních světů. Není proto divu, že různé společnosti provozující MMO hry[8] zaměstnávají za tímto účelem vyškolené ekonomy[9], neboť udržování ekonomiky, i když jen virtuální, v rovnováze

[7] Viz kapitola 2.3 Funkce peněz.

[8] MMO hra (anglicky „massively multiplayer online game) je hra, která umožňuje účast velkého počtu hráčů pomocí internetového připojení (Janssen, 2015b).

[9] Příkladem může být Yanis Varoufakis, řecký ekonom a od ledna roku 2015 i řecký ministr financí, který po nějaký čas pracoval pro americkou společnost Valve jako ekonomický konzultant (Varoufakis, 2012).

představuje obrovskou zodpovědnost. Jediná aktualizace může virtuální ekonomiku změnit zcela zásadním způsobem a třeba i znehodnotit veškerou peněžní zásobu virtuální měny.

Evropská centrální banka (2012) uvádí dva možné způsoby získávání virtuálních měn. Ten první, rychlejší, spočívá v zakoupení určitého množství virtuální měny za skutečné peníze na základě předem stanoveného směnného kurzu. Ten druhý zahrnuje účast členů virtuální komunity ve specifických aktivitách, které nabízejí odměnu za splnění daných požadavků.

3.1.3 Bitcoin jako online platební systém

Nyní zpět k Bitcoinu coby online platebnímu systému. Jeho autor, Satoshi Nakamoto, nejprve publikoval v listopadu roku 2008 dokument popisující hlavní principy fungování Bitcoinu a později, 9. ledna 2009, zveřejnil jeho první verzi (Nakamoto, 2008). Davis (2011) uvádí, že zrod Bitcoinu byl částečně Nakamotovou reakcí na nepříznivý ekonomický vývoj ke konci první dekády 21. století. Důkazem může být krátký úryvek z titulku zprávy v londýnském deníku The Times z 3. ledna 2009, který Nakamoto zakódoval do dat tzv. „genesis“ bloku – prvního bloku tzv. „block chainu“ (bude vysvětleno níže). Zpráva[10] informuje o tom, že britský kancléř Alistair Darling je nucen zvažovat druhý státní zásah na záchranu britských bank, neboť ten minulý (částečné znárodnění o objemu 37 miliard britských liber) selhal.

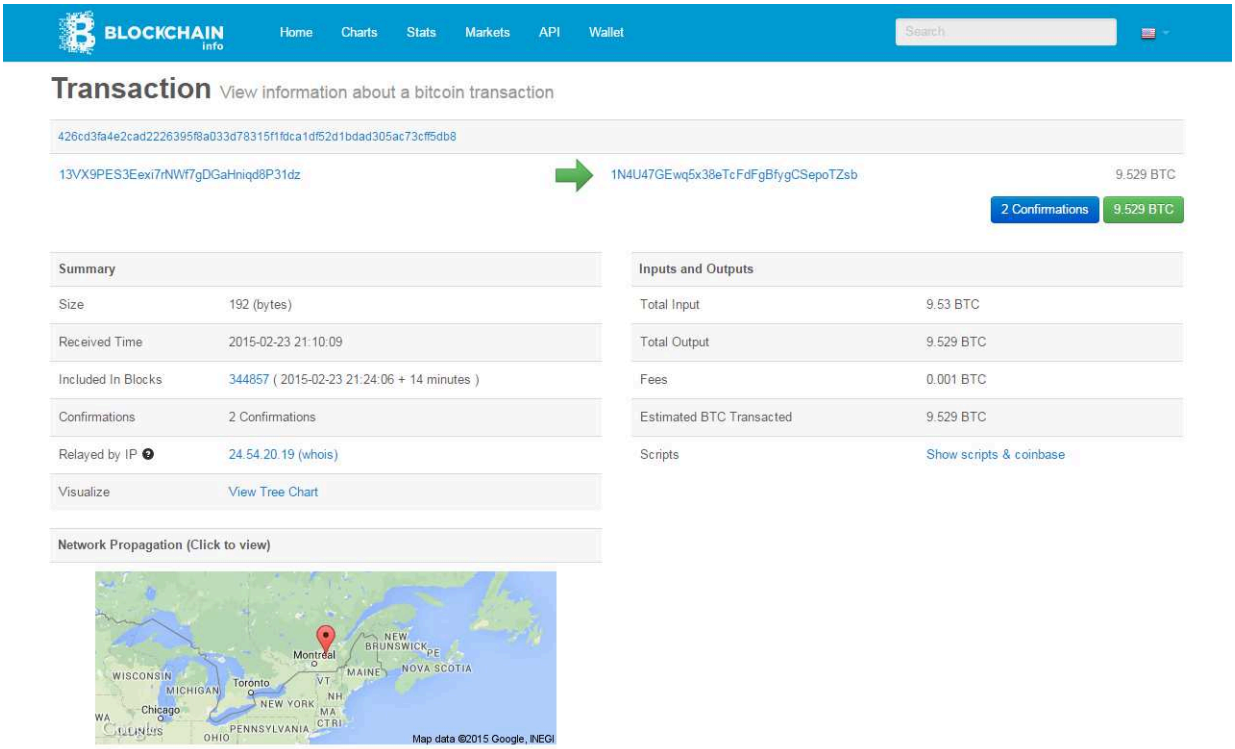
Nakamoto (2009) ve svém dokumentu poukazuje na slabiny současných elektronických platebních systémů. Problémem při zpracovávání elektronických transakcí je především závislost na existenci důvěryhodné třetí strany, nejčastěji nějaké finanční instituce (viz výše zmiňovaný aspekt centralizace). Tento princip, ačkoli funguje dostatečně pro většinu transakcí, má několik nevýhod, jež jsou charakteristické pro model založený na důvěře. Hlavní problém nastává v souvislosti s možností vrácení platby, jejíž existence pomáhá v ochraně spotřebitele. Řešení sporů v této oblasti však zvyšuje transakční náklady, které si finanční instituce kompenzují nejčastěji prostřednictvím poplatků za zprostředkování plateb. Nejen to, s možností vrácení platby jsou obchodníci nuceni mít se na pozoru před svými zákazníky a požadovat po nich více osobních informací než by jinak bylo nutné. Určité procento podvodů v takovéto situaci je považováno za nevyhnutelné.

Jako řešení těchto neduhů představil Nakamoto Bitcoin – decentralizovaný elektronický platební systém, který je založen na kryptografii namísto důvěry, a který

[10] Viz Elliot a Duncan (2009).

umožňuje kterýmkoliv dvěma stranám, jež jsou ochotny spolu obchodovat, uskutečňovat transakce přímo mezi sebou bez nutnosti zprostředkování třetí stranou. Aby bylo zabráněno vícenásobnému utracení stejných prostředků (tzv. double-spendingu) používá systém tzv. „block chain“, což je zjednodušeně řečeno distribuovaná databáze všech uskutečněných transakcí, kterou sdílejí všichni členové peer-to-peer sítě. Jak uvádí Wallace (2011), konvenční řešení tohoto problému zahrnuje existenci centrální autority, která udržuje přehled nad všemi transakcemi vedením určité formy účetní knihy. Taková účetní kniha pak zamezuje podvodům, na druhou stranu však vyžaduje důvěryhodnou třetí stranu, která zajišťuje její administraci. Davis (2011) dodává, že Nakamoto vyřešil problém double-spendingu pomocí inovativní kryptografie. Software, který Nakamoto naprogramoval, a který je volně veřejně dostupný (např. na portálu SourceForge), šifruje každou transakci takovým způsobem, že odesílatel i příjemce zůstávají anonymní. Kdokoliv tak může vidět, že určité množství bitcoinů se přesunulo od A k B, avšak A i B jsou identifikováni pouze pomocí řetězců číslic a písmen (viz obr. 3.2). Všechny transakce jsou nevratné, tudíž není možné, aby byl kterýkoli bitcoin utracen dvakrát. Kdyby se o to chtěl někdo pokusit, musel by změnit celý block chain, neboť ten je tvořen jednotkami (bloky transakcí), z nichž každá obsahuje záznam o té předchozí. To, jak uvádí Nakamoto (2009), není možné, pokud útočník nemá pod kontrolou větší výpočetní výkon, než je součet výpočetních výkonů ostatních členů sítě.

Obr. 3.2 Příklad jednoduché transakce bitcoinů



Zdroj: Blockchain (2015a)

3.1.4 Hlavní charakteristiky Bitcoinu

Otázka „Co je to Bitcoin?“ ve smyslu definování podstaty daného pojmu již byla zodpovězena (viz podkapitoly 3.1.1 a 3.1.3). Tato podkapitola bude zaměřena na popis hlavních charakteristických znaků Bitcoinu a vysvětlení hlavních rozdílů Bitcoinu oproti klasickým měnám. Konkrétně CoinDesk (2014a) uvádí tyto charakteristiky:

- Decentralizace,
- jednoduchost a dostupnost,
- rychlost,
- nízké náklady,
- anonymita,
- transparentnost,
- a nevratnost.

Hlavním a již několikrát zmiňovaným aspektem Bitcoinu je decentralizace. Je to také vlastnost, jež mnozí považují za hlavní výhodu oproti klasickým měnám. Neexistuje totiž žádná osoba, žádná instituce, dokonce ani žádná centrální autorita, která by vlastnila, řídila nebo jakkoliv ovlivňovala[11] Bitcoin. Je to pochopitelné – Davis (2011) uvádí, že jednou z příčin vzniku Bitcoinu byla zhoršená ekonomická situace ke konci první dekády 21. století způsobená kolapsem finančního systému[12]. Není proto divu, že důvěra lidí vůči finančním institucím a klasickým platebním prostředkům značně opadla. Nakamoto se tak snažil vytvořit měnu, která by byla odolná jak vůči nepředvídatelným opatřením monetární politiky centrální autority, tak i proti chamtivosti a bezohlednosti bankéřů a politiků. A to se mu vskutku povedlo, síť Bitcoinu je tvořena pouze jeho uživateli a emise nových bitcoinů je založená na matematických zákonitostech a plně řízená Bitcoin softwarem. CoinDesk (2014a) upřesňuje, že do roku 2140 má do oběhu postupně vejít celkem 21 milionů bitcoinů, přičemž tempo jejich uvolňování je dáno výší odměny za každý nový blok (bude vysvětleno později). Tato odměna činí aktuálně (březen 2015) 25 bitcoinů a má se snižovat na polovinu přibližně každé 4 roky.

Jednoduchost Bitcoinu spočívá v jeho uživatelsky pohodlném prostředí. Pro posílání a přijímání transakcí stačí mít tzv. Bitcoin peněženku. CoinDesk (2014b) uvádí několik

[11] Technicky vzato, na Bitcoinu neustále pracují týmy vývojářů, kteří se snaží vylepšovat a zdokonalovat existující protokol, avšak záleží pouze na uživatelích, kterou verzi se rozhodnou používat. Bitcoin funguje, pouze když všichni uživatelé používají software se stejnými zákonitostmi. Snahou vývojářů je tedy dosáhnout konsenzu mezi všemi uživateli (Bitcoin.org, 2015a).

[12] Není nelogické předpokládat, že tato situace určitým dílem přispěla k rozšíření i relativně velkému úspěchu Bitcoinu.

variant s různým stupněm bezpečnosti, přičemž zřízení takové peněženky nejjednodušším (technicky ale také nejméně bezpečným) způsobem nezabere víc než pár vteřin a vyžaduje po uživateli pouze volbu hesla[13]. To je od založení např. běžného bankovního účtu obrovský rozdíl. Pro uskutečnění transakce je pak nutné znát pouze adresu peněženky příjemce.

Bitcoin.org (2015a) uvádí, že Bitcoin je rovněž charakteristický svou dostupností. Platby v rámci Bitcoinu lze uskutečnit z kteréhokoliv místa na světě v jakoukoliv dobu. Na rozdíl od platebních karet či bankovních účtů také neexistuje žádný limit, který by omezoval výši transakcí. S tím souvisí také další dva důležité znaky Bitcoinu – rychlost a nízké náklady. Každá transakce musí být zaznamenána do block chainu, proto doba, kterou trvá poslat někomu bitcoiny závisí na zpracování aktuálně posledního bloku transakcí sítí Bitcoin. To obyčejně trvá kolem 10 minut. Uživatelé si přitom mohou vybrat, zda zaplatí minimální nebo žádné poplatky. Přiloží-li uživatel k transakci poplatek, zvyšuje to její prioritu při zpracování sítí a vyúsťuje v rychlejší připsání bitcoinů do peněženky příjemce. Například transakce na obr. 3.2 ve výši 9,53 bitcoinů obsahuje poplatek o velikosti jedné tisíciny bitcoinu.

Jak již bylo zmíněno v podkapitole 3.1.3, Bitcoin je anonymní. Kdokoliv může vidět, z jaké adresy a kam se přesunulo kolik bitcoinů, avšak neexistuje žádný způsob jak zjistit komu, která adresa patří. Uživatelé, kteří vyžadují extra stupeň soukromí, mají možnost vytvořit si několik adres, nebo svou adresu pravidelně měnit.

Aspekt transparentnosti Bitcoin naplňuje tím, že jeho software je kompletně open-source – jeho zdrojový kód je veřejně dostupný, to znamená, že kdokoli s potřebnými znalostmi může ověřit a přesvědčit se, zda vše funguje tak jak má. To samé platí o transakcích, ty se uskutečňují bez účasti jakékoliv třetí strany a všechny jsou zaznamenány do již zmiňovaného block chainu, který je sdílený všemi uživateli sítě. Je tedy zřejmé, že na rozdíl od systému postaveného na důvěře lidí vůči bankám, nepotřebuje Bitcoin ke svému fungování důvěru vůbec žádnou.

V neposlední řadě jsou Bitcoin transakce charakteristické svou nevratností. Jakmile uživatel pošle své bitcoiny jinému uživateli, už je zpátky nedostane, ledaže by mu je příjemce poslal. Tím se Bitcoin odlišuje od služeb typu PayPal, kde uživatel může požádat o vrácení transakce (tzv. „chargeback“).

Z výše uvedeného by se mohlo zdát, že Bitcoin představuje ideální a téměř dokonalý systém pro placení za jakékoliv zboží a služby a neexistuje žádný rozumný důvod proč jej nepoužívat. Bohužel není tomu tak, Bitcoin s sebou přináší i některé nevýhody, jak uvádí

[13] Platí v případě založení Bitcoin peněženky (nejen) přes službu Blockchain.info. U jiných zprostředkovatelů může být vyžadována např. emailová adresa nebo jméno.

Bitcoin.org (2015a). Za prvé mnozí lidé nemají o Bitcoinu ponětí, nebo jej z různých důvodů nepoužívají. Zdaleka ne každý obchodník je ochoten akceptovat bitcoiny jako platbu za své zboží a služby, což činí použití Bitcoinu v takovýchto situacích jako problematické. Za druhé hodnota 1 bitcoinu v čase z různých důvodů značně kolísá, dlouhodobá držba bitcoinů s sebou proto nese pocit nejistoty. Z teoretického hlediska lze říct, že funkce uchovatele hodnoty není v případě Bitcoinu zcela naplněna, podobně jako funkce prostředku směny. Za třetí je nutné připomenout stále probíhající vývoj. Bitcoin stále není ve své finální fázi a na spoustě atributů se stále pracuje.

3.2 Satoshi Nakamoto

S fenoménem Bitcoin je neoddělitelně spojeno jméno jeho autora – Satoshiho Nakamota. Kdo to vůbec je? Tuto otázku si již dlouhou dobu klade mnoho lidí, avšak Nakamotova identita zůstává opředena tajemstvím. Tato kapitola bude věnována právě této záhadné postavě a její klíčové roli ve vývoji Bitcoinu.

Wallace (2011) i CoinDesk (2015) uvádí, že jméno Satoshi Nakamoto se poprvé objevuje v korespondenci malé a relativně uzavřené komunity lidí zabývající se kryptografií 1. listopadu roku 2008. Nakamoto, o němž nikdo z příjemců korespondence do té doby nikdy neslyšel, tehdy ve svém emailu uvedl odkaz na svůj výzkumný dokument pojmenovaný „Bitcoin: A Peer-to-Peer Electronic Cash System“. V něm nastínil svou ideu nové digitální měny založené na kryptografii – věc, o jejíž vynalezení tito lidé usilovali po celá desetiletí. Tím na sebe logicky upoutal nemalou pozornost, jež se brzy změnila v obrovský zájem o zjištění jeho pravé identity. Wallace (2011) je přesvědčen, že Satoshi Nakamoto je pouhý pseudonym, a je pravděpodobnější, že se pod ním skrývá spíše skupina lidí, než jeden šestatřicetiletý člověk pocházející z Japonska, jak o sobě na svém profilu Nakamoto uváděl.

Lidé se od té doby snažili odhalit Nakamotovu pravou identitu celou škálou různých metod, od těch relativně legitimních až po ty, které hraničí s konspiračními teoriemi. Například Davis (2011) založil svůj výzkum na lingvistické analýze veškerého textu, co se kdy na Internetu objevil pod Nakamotovým jménem. Podle jeho závěrů šlo o člověka britské nebo irské národnosti s rozsáhlými znalostmi v oblasti kryptografie, programování v jazyce C++ a ekonomie. Podle Nakamotova vztahu ke komunitě zabývající se kryptografií Davis (2011) předpokládal, že bude jedním z účastníků konference „Crypto 2011“, konající se každoročně ve městě Santa Barbara v Kalifornii. Na základě tohoto úsudku nejprve považoval za Nakamota třiadvacetiletého Michaela Cleara, studenta teoretické kryptografie na Trinity

College v Dublinu. Potom co Clear popřel, že by měl se Satoshim cokoliv společného, odkázal Davisovu pozornost na jednatřicetiletého finského výzkumníka z Institutu pro informační technologie v Helsinkách, jménem Vili Lehdonvirta. Ten rovněž jakoukoliv spojitost s Nakamotem odmítl.

Den na to co Davis (2011) zveřejnil svůj článek, zkritizoval jeho práci Penenberg (2011). Podle jeho názoru text, podle kterého Davis usoudil, že Satoshi Nakamoto pochází odněkud z Britských ostrovů, byl záměrně konstruován tak, aby vytvářel iluzi, že jde o rodilého britského, resp. irského mluvčího. Penenberg (2011) proto založil svoji metodu na extrahování různých frází z již výše zmíněného Nakamotova výzkumného dokumentu. Pomocí internetového vyhledávače pak zjišťoval, jestli se některá fráze nevyskytla již dříve v nějakém jiném dokumentu. Překvapivě uspěl, konkrétně s frází „computationally impractical to reverse“, kterou objevil v žádosti o patent[14] na aktualizaci a distribuci šifrovacích klíčů (Updating and Distributing Encryption Keys), technologii podobnou té kterou využívá Bitcoin. Čirou náhodou tato žádost byla podána 15. srpna 2008, přesně tři dny před zaregistrováním domény bitcoin.org. Penenberg (2011) tak došel k závěru, že Satoshi Nakamoto jsou (nebo s ním mají něco společného) autoři dané žádosti o patent, Neal King, Vladimir Oksman a Charles Bry. Tvrzení podepřel tím, že doména bitcoin.org byla registrována ve Finsku, kam 6 měsíců předtím cestoval Bry. CoinDesk (2015) tuto teorii vyvrací tím, že doména bitcoin.org byla ve skutečnosti zaregistrována pomocí japonské anonymní registrační služby a až později, 18. května 2011, byla registrace převedena do Finska. Všichni tři také jakoukoliv spojitost s Nakamotem odmítají.

CoinDesk (2015) uvádí velké množství dalších jmen, jež byla v průběhu posledních několika let uváděna jako potenciální pojítko se Satoshim. Nejčastěji se mezi nimi objevují jména bývalých vývojářů nebo jiných osob, kteří s Nakamotem spolupracovali na vývoji Bitcoinu v jeho raných počátcích, jako třeba Martti Malmi, finský vývojář, který vyvinul první uživatelské rozhraní Bitcoinu, švýcar Michael Weber nebo američan Hal Finney, příjemce historicky první transakce bitcoinů na světě.

Goodmanová (2014) vydala v březnu roku 2014 článek v časopise Newsweek, ve kterém tvrdí, že úspěšně vystopovala reálného Satoshiho Nakamota. Podle ní stojí za zrodem Bitcoinu čtyřiašedesátiletý Američan s japonskými kořeny žijící ve skromném obydlí v Temple City v Kalifornii, jehož celé jméno je Dorian Satoshi Nakamoto. Podle slov příbuzných pracoval po nějakou dobu na utajených záležitostech pro velké korporace a

[14] Viz King, Oksman a Bry (2008).

americkou armádu. Palmer (2014) uvádí, že Dorian Nakamoto na článek zareagoval tím, že prostřednictvím svého právního zástupce vydal veřejné prohlášení, ve kterém bezpodmínečně popírá reportáž Goodmanové. Tvrdí, že termín Bitcoin slyšel poprvé v únoru 2014, a že nedisponuje žádnými znalostmi v oblasti kryptografie, P2P sítí nebo alternativních měn.

Coindesk (2015) uvádí, že nikdo nemůže s jistotou říct, kdo ve skutečnosti Satoshi Nakamoto je a co v současné době dělá. V jednom ze svých posledních emailů z dubna 2011 se zmínil, že už se Bitcoinem dále nezabývá a že projekt je v dobrých rukou. Wallace (2011) poznamenává, že Nakamoto se vytratil stejně tajemně, jako se objevil. Nezáleží však na postavách, které stojí za vznikem Bitcoinu, ale na Bitcoinu samotném. Davis (2011) dodává, že Nakamotova identita by ani neměla být důležitá. Jeho systém byl postaven tak, aby nebylo třeba důvěřovat žádnému jednotlivci ani žádné korporaci či vládě.

3.3 Těžba

V případě klasických forem peněz dochází k jejich emisi z největší části prostřednictvím poskytování úvěrů obchodními bankami nebankovním subjektům, jak bylo uvedeno v kapitole 2.5. V případě Bitcoinu ale neexistují žádné instituce, které by měly možnost podobným způsobem zvyšovat zásobu bitcoinů. Nové bitcoiny však stále přibývají a jejich počet se postupně zvyšuje. Čím je to způsobeno? Odpověď představuje právě proces těžby, jenž je předmětem této kapitoly.

Pro proces těžby bude ze všeho nejdřív nutné přesněji definovat již dříve zmiňovaný pojem „block chain“, neboť jeho dosud vágní pojetí nebude již dále dostačující. Block chain je, jak už doslovný překlad jeho názvu napovídá, řetězec bloků. Bitcoin.org (2015b) uvádí, že každý blok obsahuje záznamy transakcí v určité formě a tzv. „hash“ předchozího bloku, jež umožňuje zapojovat jeden blok za druhým. CoinDesk (2014d) uvádí, že hash je produktem hashovací funkce, tj. algoritmu, který dokáže transformovat různě velké objemy dat na stejně velké zdánlivě náhodné sekvence písmen a číslic. Hash má ještě několik dalších klíčových vlastností:

- Je relativně jednoduché vytvořit hash ze vstupních dat, je ale prakticky nemožné z hashe rekonstruovat původní vstupní data.
- Každý hash je unikátní, to znamená, že:
    - Neexistuje stejný hash pro dva různé objemy vstupních dat,
    - a jakoukoliv změnou ve vstupních datech dojde k vytvoření úplně nového zcela odlišného hashe.

Co to znamená pro block chain? Tím, že každý blok transakcí obsahuje také hash předchozího bloku vzniká uspořádaný a časově seřazený seznam všech uskutečněných transakcí[15] (připomínající účetní knihu). Pokud by chtěl někdo změnit některou transakci, nejen že by se změnil hash bloku, ve kterém byla transakce obsažena, ale změnily by se i hashe ostatních po něm následujících bloků. Všichni účastníci sítě by hned viděli, že se někdo pokusil o podvod, neboť block chain je sdílený mezi všemi.

Vytěžení bitcoinů představuje úspěšné připojení nového bloku transakcí k block chainu. Tuto činnost vykonávají tzv. „těžaři", jež mezi sebou soutěží. Těžař, který jako první vyřeší blok splněním určitých podmínek (vysvětleno dále), inkasuje odměnu ve výši 25 bitcoinů[16] plus sumu poplatků přiložených k jednotlivým transakcím v daném bloku. To dává těžařům motivaci vynakládat stále větší výpočetní výkon na řešení bloků, zajišťuje fungování transakcí, a udržuje Bitcoin v chodu.

Vyřešení bloku a vytěžení bitcoinů však není jednoduchá záležitost. Bitcoin.org (2015b) uvádí, že Bitcoin vyžaduje, aby každý blok byl důkazem toho, že k jeho vytvoření bylo potřeba investovat určité množství výpočetního výkonu. To zajišťuje, aby nepoctiví členové sítě, jež se snaží o modifikaci minulých bloků, museli vždy vynaložit větší úsilí než ti poctiví, kteří usilují pouze o připojení dalšího bloku do block chainu. Řetězení bloků pomocí hashů způsobuje, že náklady na modifikaci určitého bloku narůstají s každým novým připojeným blokem. Tento princip bývá označován termínem „proof of work". Jak ale těžař prokáže, že opravdu vykonal potřebnou práci, že obětoval určitý výpočetní výkon na vyřešení bloku? CoinDesk (2014d) uvádí, že Bitcoin neakceptuje jen tak ledajaký hash, ale stanovuje požadavky, které musí každý hash bloku, který aspiruje na připojení k ostatním, splňovat. Žádným způsobem totiž nelze předpovědět, jak bude hash vypadat, dokud jej hashovací algoritmus nedokončí. Dosud byly zmíněny pouze dvě části, jež jsou používány k vytvoření hashe – hash předchozího bloku a hash transakcí. Existuje však ještě třetí, klíčová část a tou je tzv. „nonce". Nonce představuje náhodně vygenerovaná data, která jsou měněna při každém pokusu o vyprodukování hashe. Nevyhovuje-li výsledný hash formátu stanoveném Bitcoinem, vygeneruje se nová nonce a celý proces se opakuje znovu. Těžař, který jako první najde nonci, pomocí které je vytvořen vyhovující hash, připojí nový blok do block chainu a dá o tom vědět všem ostatním účastníkům sítě.

[15] Aktuální velikost block chainu (k 11. březnu 2015) činí přibližně 30 GB a každým dnem se zvyšuje přibližně o 55 MB (Blockchain, 2015b).

[16] Aktuálně (k 11. březnu 2015) je platná tato hodnota, avšak přibližně každé 4 roky dochází k poklesu odměny na jednu polovinu původní hodnoty. Očekává se, že k dalšímu poklesu dojde někdy v polovině roku 2016. Potom co bude do oběhu uvolněno všech 21 milionů bitcoinů bude jako iniciativa k těžbě sloužit místo pevně stanovené odměny pouze suma poplatků u transakcí.

CoinDesk (2013) uvádí, že k zajištění hladkého průběhu tohoto procesu používají těžaři v současné době speciálně navržený software běžící na vysokovýkonných počítačích používajících periferie designované striktně na těžbu bitcoinů. Tyto periferie používají technologii, jež nese název ASIC, což je zkratka pro „Application Specific Integrated Circuit“. Zjednodušeně řečeno se jedná o integrovaný obvod, jenž je navržen i vyráběn pouze pro jednu specifickou aplikaci. To umožňuje dosahovat maximálního výpočetního výkonu při relativně nízké spotřebě elektrické energie. Stejně jako například při těžbě ropy, je totiž důležité, aby náklady na těžbu nepřesáhly zisk z vytěžené suroviny. Ještě v nedávné minulosti bylo možné těžit bitcoiny i na obyčejných stolních počítačích využitím výpočetního výkonu procesoru či grafické karty. V současné době je však tato technologie již značně zastaralá a neefektivní. Navíc s rozvojem Bitcoinu došlo také ke vzniku zcela nového odvětví firem, jejichž hlavní specializací je právě výroba čipů na těžbu bitcoinů používajících technologii ASIC. Tyto firmy se doslova předhánějí v tom, která z nich uvede na trh nejvýkonnější čip s nejnižší spotřebou.

3.4 Transakce

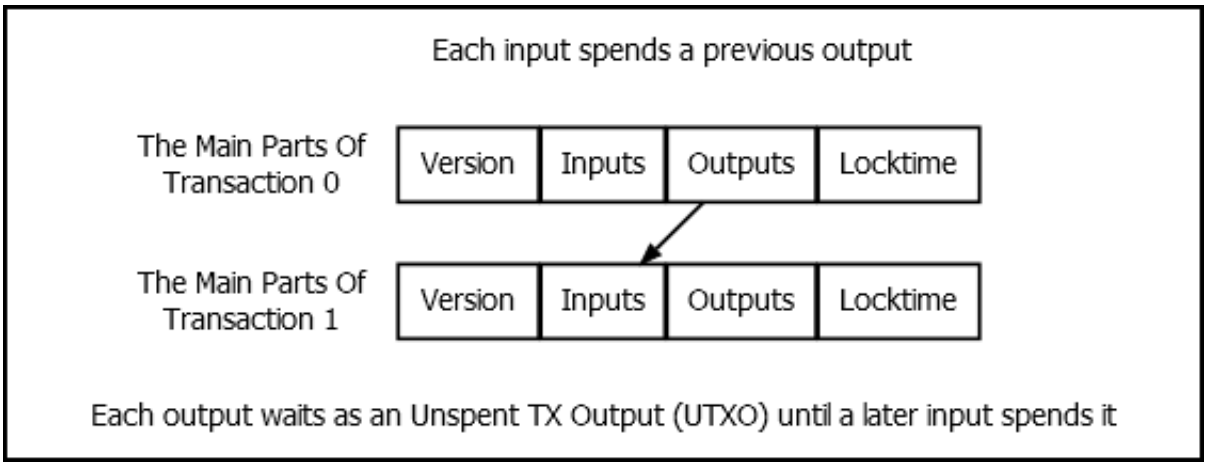
Má-li být Bitcoin vůbec považován za formu digitálních peněz, musí plnit funkci zprostředkovatele směny. Jeho existence by byla zbytečná, kdyby neumožňoval svým uživatelům vydávat a přijímat platby za zboží a služby. Proto hlavní hybnou silou Bitcoinu jsou právě transakce, které umožňují jeho uživatelům utrácet své prostředky uložené v Bitcoin peněženkách (zmiňovaných v podkapitole 3.1.4). Avšak termín „uložené“ není úplně správný. V této kapitole bude daná problematika uvedena na pravou míru a budou zhruba vysvětleny principy, na kterých funguje mechanismus transakcí.

Standardní formy peněz mohou být uloženy například na bankovních účtech, v trezorech bank či v peněženkách jednotlivců. S tím kontrastuje Bitcoin, jak uvádí CoinDesk (2014c) – bitcoiny ve skutečnosti neexistují a proto nemohou být nikde uloženy. Není to totiž potřeba, neboť v block chainu existují záznamy všech transakcí mezi jednotlivými adresami (peněženkami). Každý bitcoin lze tak vystopovat napříč block chainem až k jeho samotnému vzniku vyplacením odměny těžaři, který jej úspěšně vytěžil. Tímto způsobem se dá zjistit jaké množství bitcoinů patří ke každé adrese.

Bitcoin.org (2015b) uvádí, že každá transakce se skládá z několika částí (viz schéma na obr. 3.3), které umožňují provádět jednoduché přímé platby, ale i komplexní transakce. Každá transakce obsahuje vždy alespoň jeden vstup (Input) a jeden výstup (Output), přičemž

každý vstup je výstupem nějaké jiné předchozí transakce. Každý výstup je uložený do block chainu jako neutracený výstup transakce (Unspent Transaction Output, zkr. UTXO) a čeká se, dokud ho „neutratí“ některý vstup. Vlastní-li někdo 1 bitcoin, znamená to, že má k dispozici 1 bitcoin čekající v jednom nebo více neutracených výstupech transakcí.

Obr. 3.3 Hlavní části transakce



Zdroj: Bitcoin.org (2015b)

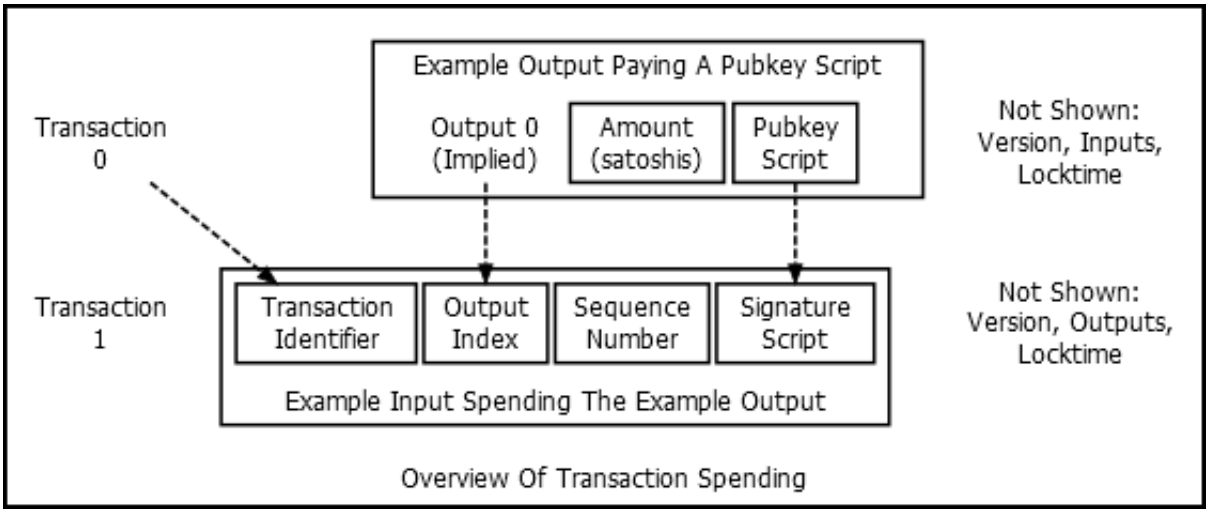
Další částí je číslo verze transakce (Version). Tato část pomáhá k identifikaci souboru pravidel, která mají být sítí použita pro autorizování transakce. Vývojářům Bitcoinu to umožňuje vytvořit čas od času nový lehce pozměněný soubor pravidel, bez toho aniž by se staré transakce staly neplatnými. Poslední částí je Locktime - časový zámek, kterým může transakci opatřit uživatel. Tento časový zámek udává, kdy nejdřív může být transakce přidána do block chainu. To znamená, že utracení výstupu transakce bude možné až po uplynutí určité doby. Rozmyslí-li si uživatel transakci s časovým zámkem, může vytvořit novou transakci (bez časového zámku), ve které použije stejný vstup jako v transakci s Locktime (tj. vytvoří celkem 2 transakce, jejichž vstupem je tentýž UTXO nějaké jiné předchozí transakce). Přidání druhé transakce do block chainu učiní transakci s časovým zámkem neplatnou, neboť každý UTXO může být utracen pouze jednou. Jinými slovy, vstupy platné transakce mohou být pouze neutracené výstupy předchozích transakcí.

Jak uvádí CoinDesk (2014c), často se stává, že hodnoty výstupů a vstupů (v bitcoinech) se neshodují. Příkladem může být situace, kdy uživatel A chce zaplatit uživateli B 4,2 bitcoinu, ale pro vytvoření transakce má k dispozici pouze neutracené výstupy v hodnotách 1, 2 a 3 bitcoiny. Nejen že žádný výstup neodpovídá požadované hodnotě vstupu, ale ani sečtením kterýchkoliv dvou výstupů nelze vytvořit přesně požadovanou výši vstupu.

Navíc platí, že žádný UTXO nemůže být rozdělen. Jediným řešením je v tomto případě vytvoření transakce se dvěma vstupy (výstupy ve výši 2 a 3 bitcoiny) a dvěma výstupy – jeden ve výši 4,2 bitcoinu (platba uživateli B) a druhý ve výši 0,8 bitcoinu[17]. Tento výstup je poslán zpět na adresu uživatele A a představuje „vrácení drobných". V konečném výsledku má uživatel A k dispozici dva neutracené výstupy o hodnotách 1 a 0,8 bitcoinu, a uživatel B jeden UTXO ve výši 4,2 bitcoinu (za předpokladu, že předtím neobdržel platby od žádných dalších uživatelů).

Zbývá vysvětlit pouze mechanismus autorizace transakcí. K tomu poslouží bližší pohled na vstupy a výstupy a jejich části (viz schéma na obr. 3.4). Bitcoin.org (2015b) uvádí, že každý výstup (Output) má index, podle kterého je identifikován, a přesně stanovenou hodnotu[18] (Amount) vázanou na tzv. „Pubkey script". Hlavní charakteristikou tohoto Pubkey skriptu je, že kdokoliv kdo splní podmínky dané tímto skriptem je oprávněn utratit hodnotu na něj vázanou. Naproti tomu částmi vstupu (Input) jsou identifikátor transakce (Transaction Identifier), číslo indexu výstupu (Output Index), tj. část, která identifikuje výstup určený k utracení, sekvenční číslo[19] (Sequence Number) a tzv. „Signature Script", jenž poskytuje data, která uspokojí požadavky dané Pubkey skriptem.

Obr. 3.4 Jednotlivé části vstupu a výstupu transakce



Zdroj: Bitcoin.org (2015b)

[17] Hodnota tohoto druhého výstupu bude pravděpodobně nižší než 0,8 bitcoinu, neboť většina transakcí obsahuje nepatrný poplatek v řádech sta miliontin až tisícin bitcoinu.

[18] Tato hodnota není uvedena v bitcoinech, nýbrž v jednotkách zvaných „satoshi" (v češtině též „satoši") – 1 satoshi představuje 0,00000001 (tj. 10^{-8}) bitcoinu a je to nejmenší jednotka, na kterou lze bitcoin rozdělit.

[19] Sekvenční číslo je pozůstatkem staré verze Bitcoinu a pro vysvětlení principů autorizace transakcí není důležité. Jeho funkci v současné době vykonává jiná část transakce – Locktime.

Předtím než bude moct uživatel A poslat uživateli B určitý obnos je nutné, aby uživatel B nejdříve vygeneroval soukromý a veřejný klíč. Soukromý klíč jsou náhodně vygenerovaná data, jejichž kopie je pomocí algoritmu transformována na veřejný klíč. Tento veřejný klíč je dále pomocí kryptografie šifrován na tzv. „hash“ veřejného klíče. Adresa Bitcoin peněženky, kterou uživatel B sdělí uživateli A, je zakódovaný hash veřejného klíče. Má-li uživatel A adresu peněženky uživatele B, může vytvořit transakci s výstupem opatřeným specifickými instrukcemi. Utratit výstup této transakce umožní tyto instrukce pouze tomu, kdo se prokáže soukromým klíčem, jež odpovídá hashi veřejného klíče uživatele B. Tyto instrukce jsou nazývány „Pubkey script“ (zmiňovaný výše). Transakce je pak od uživatele A vyslána napříč celou Bitcoin sítí a přidána do block chainu. Síť zaznamená nový UTXO a peněženka uživatele B zobrazí aktivní zůstatek (neboť jen ta obsahuje soukromý klíč uživatele B).

Rozhodne-li se uživatel B tento nový zůstatek utratit, vytvoří transakci se vstupem, jež odkazuje (identifikátorem transakce) na hash transakce vytvořenou uživatelem A, a na příslušný výstup (číslem indexu výstupu). Pak už jen doplní svůj Signature skript, jenž poskytne data potřebná pro splnění podmínek, které stanovil uživatel A ve výstupu předchozí transakce ve formě Pubkey skriptu, a transakce je autorizována.

3.5 Dílčí shrnutí

Na začátku této části práce bylo vysvětleno co je to Bitcoin a byly zde také uvedeny 2 různá hlediska na definici Bitcoinu. Bitcoin je nutné chápat jako online platební systém založený na principu peer-to-peer sítě a rovněž jako decentralizovanou digitální měnu používanou v tomto systému. Bitcoin je specifickým typem digitální měny, jež používá kryptografii (šifrování) k zabezpečování transakcí a k řízení emise nových jednotek. Digitální měna představuje peníze uchovávané a převáděné elektronicky. Do kategorie digitálních měn spadají také virtuální měny, od nich se však Bitcoin výrazně liší aspektem centralizace. Bitcoin co by online platební systém byl navržen tak, aby neobsahoval slabiny, jimiž se vyznačují některé současné elektronické platební systémy. Jeho hlavní předností je nezávislost na jakékoli centrální autoritě a umožnění kterýmkoliv dvěma stranám, jež jsou ochotny spolu obchodovat, uskutečňovat transakce přímo mezi sebou. Problému vícenásobného utrácení Bitcoin předchází pomocí block chainu – distribuované databáze všech uskutečněných transakcí, kterou sdílejí všichni členové peer-to-peer sítě. Hlavními

charakteristikami Bitcoinu jsou decentralizace, jednoduchost a dostupnost, rychlost, nízké náklady, anonymita, transparentnost a nevratnost.

Dále následovala kapitola o autorovi Bitcoinu, Satoshi Nakamotovi. Jeho pravá identita není známa, přestože se o její odhalení pokoušelo již mnoho lidí, převážně žurnalistů. Existují domněnky, že jde o pseudonym, za kterým se skrývá skupina lidí. Nakamoto o sobě dal poprvé vědět 1. listopadu roku 2008 v souvislosti s vydáním svého výzkumného dokumentu „Bitcoin: A Peer-to-Peer Electronic Cash System“. Nakamotova konverzace s ostatními vývojáři Bitcoinu ustala v dubnu 2011 po tom, co uvedl, že Bitcoinem už se dále nezabývá a že projekt je v dobrých rukou.

Předmětem další kapitoly byla těžba bitcoinů. Tento proces spočívá ve zpracování bloku transakcí a jeho připojení do block chainu. Hlavním pilířem těžby jsou tzv. „těžaři“, kteří mezi sebou soutěží. Jejich úkolem je najít náhodně vygenerovaný řetězec dat zvaný nonce, který společně s hashem předchozího bloku a hashem transakcí vytvoří výsledný hash splňující podmínky stanovené Bitcoinem. Hash je produktem algoritmu, který dokáže transformovat různě velké objemy dat na stejně velké zdánlivě náhodné sekvence písmen a číslic. Motivací těžařů je odměna za vyřešení bloku ve výši 25 bitcoinů plus suma poplatků přiložených k jednotlivým transakcím v daném bloku. V současnosti používají těžaři k těžbě bitcoinů speciálně navržený software běžící na vysokovýkonných počítačích používajících periferie založené na technologii ASIC.

V závěrečné kapitole této části byly vysvětleny principy, na kterých funguje mechanismus transakcí. K tomu dopomohl bližší pohled na jednotlivé části transakce, jimiž jsou vstup, výstup, číslo verze transakce a tzv. „Locktime“. Každý vstup je výstupem nějaké jiné předchozí transakce. Každý výstup je nejdříve uložený do block chainu jako neutracený výstup transakce a čeká se, dokud ho „neutratí“ některý vstup. Jsou-li hodnoty výstupu a vstupu nekompatibilní, jsou vytvořeny dva výstupy, z nichž jeden představuje „vrácení drobných“ plátci transakce. Pro uskutečnění transakce je nutné, aby příjemce nejdříve vygeneroval soukromý a veřejný klíč. S pomocí zakódovaného hashe veřejného klíče příjemce může plátce vytvořit transakci s takovým výstupem, který bude moct být utracen pouze příjemcem prostřednictvím jeho soukromého klíče.

4 Cena Bitcoinu na finančních trzích

Primárním účelem Bitcoinu bylo již od samého počátku umožnit provádění transakcí mezi dvěma stranami, bez participace třetí strany (jako je stát, banka či korporace). V poslední době se však ukazuje, že Bitcoin představuje i zajímavou investiční příležitost, čehož využívá čím dál více investorů. Absence úrokové míry ovšem znamená, že jedinou formou výnosů pro investory jsou zisky z pohybů ceny Bitcoinu. A právě cena Bitcoinu a faktory, které ji ovlivňují, budou hlavním předmětem této části práce. Bude zde vycházeno z teoretických i empirických poznatků uvedených v dostupné literatuře a bude empiricky ověřena jejich platnost.

Od okamžiku vytěžení prvního bitcoinu uběhlo teprve jen něco málo přes šest let, jeho hodnota však za tu dobu prošla drastickými změnami. Z těchto šesti let je navíc ještě nutné odečíst prvních 20 měsíců, během kterých Bitcoin neměl žádnou hodnotu. Nejvolatilnějším obdobím vývoje ceny Bitcoinu byl však jednoznačně rok 2013, ve kterém se hodnota 1 bitcoinu pohybovala nahoru a dolů jako na horské dráze a na krátký čas také dosáhla svého historického maxima přesahující hodnotu 1 000 USD. To samozřejmě přilákalo obrovskou pozornost médií a Bitcoin se také čím dál častěji stával předmětem různých akademických studií, které se snažily odhalit příčiny tohoto vývoje.

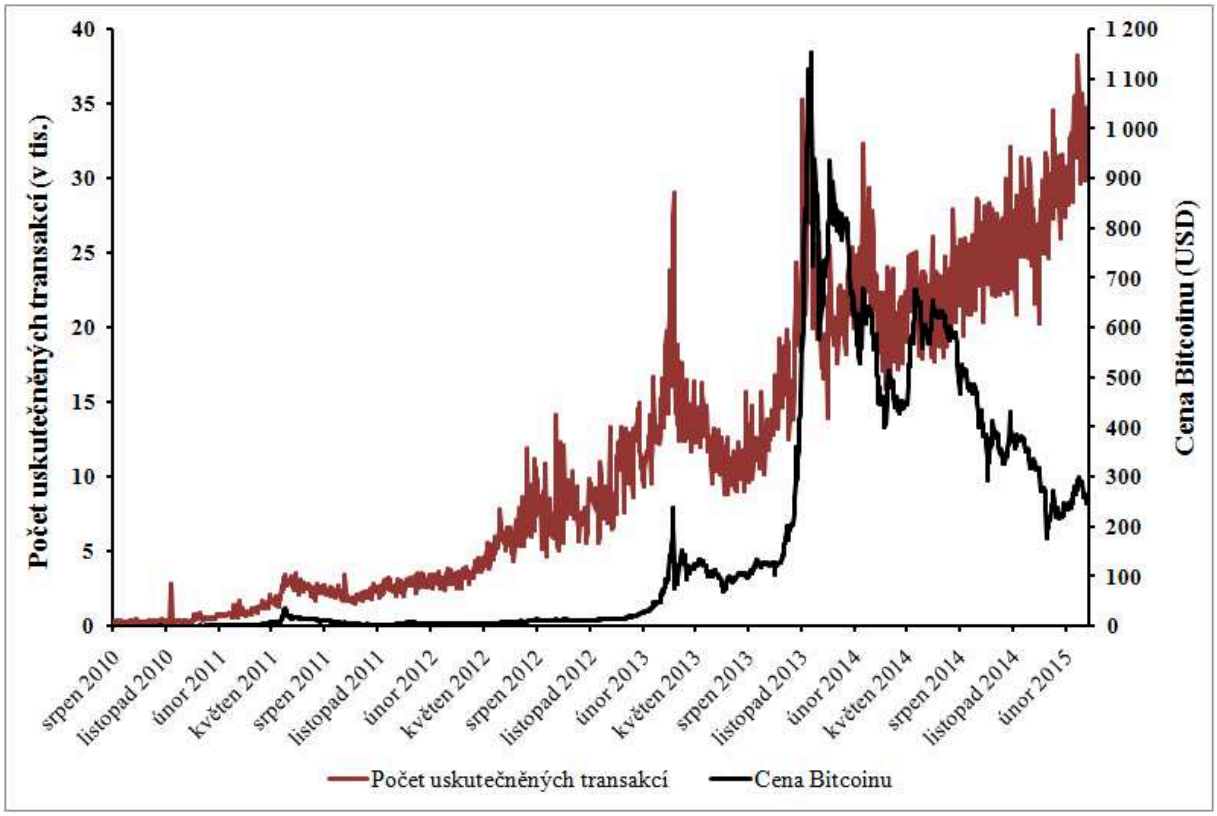
Například Buchholz, Delaney, Warren, a Parker (2012) jsou toho názoru, že hlavním činitelem v procesu utváření ceny Bitcoinu je interakce tržních sil, nabídky a poptávky. Kristoufek (2013) popírá, že by se vývoj ceny Bitcoinu dal vysvětlit základními tržními mechanismy, a namísto toho spatřuje klíčovou roli v atraktivitě Bitcoinu pro investory. Dále van Wijk (2013) se zaměřuje na hledání vztahů mezi cenou Bitcoinu a různými finančními a makroekonomickými ukazateli a Ciaian, Rajčániová a Kancs (2014) se snaží analyzovat všechny tyto faktory současně.

Většina autorů však prováděla svoji analýzu před téměř dvěma roky, což v případě vysoce dynamického vývoje, kterým Bitcoin prošel a v současnosti stále prochází, představuje dávnou minulost. Asi hlavním důvodem pro pochyby o relevantnosti předchozích výsledků výzkumů je velký cenový skok, který Bitcoin zaznamenal na přelomu listopadu a prosince roku 2013, jak ilustruje graf 4.1. Pro pochopení příčin tohoto gigantického cenového nárůstu je nutné se zaměřit na události, které nastaly během podzimu roku 2013[20]. Do té doby

[20] Pro úplnost, v tomto období (přesněji 14. října 2013) také začal největší čínský internetový vyhledávač Baidu přijímat Bitcoin jako možnost platby za služby na ochranu webových stránek před různými typy útoků (Urquhart, 2013). Není úplně jasné, jak velký vliv tato událost měla na rekordní růst ceny Bitcoinu, který nastal o měsíc později, je však možné toto považovat za jeden z počátků obrovské popularity Bitcoinu v Číně v současné době.

převažovalo mínění, že díky anonymitě uživatelů je Bitcoin velmi atraktivní pro zločince. Zásluhu na tom měla především existence stránky Silk Road, která umožňovala za bitcoiny nakupovat a prodávat různé druhy drog. Jak uvádí Greenberg (2013), 1. října 2013 americká FBI ukončila fungování Silk Road a zatkla Rosse Williama Ulbrichta, devětadvacetiletého muže považovaného za zakladatele a vlastníka tohoto nelegálního internetového tržiště, který byl následně obviněn z obchodování s narkotiky, praní špinavých peněz a počítačového hackingu. V reakci na to se o měsíc a půl později konalo slyšení v senátu Spojených států na téma „Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies“. Bylo to poprvé v historii, co se americká vláda začala vážně zajímat o digitální měny a o jejich přínosy a nástrahy. Obrovská pozornost médií a veřejnosti pak měla za následek bezprostřední raketový vzestup ceny Bitcoinu až na hodnotu přesahující 1 000 USD.

Graf 4.1 Historický vývoj ceny Bitcoinu a množství provedených transakcí



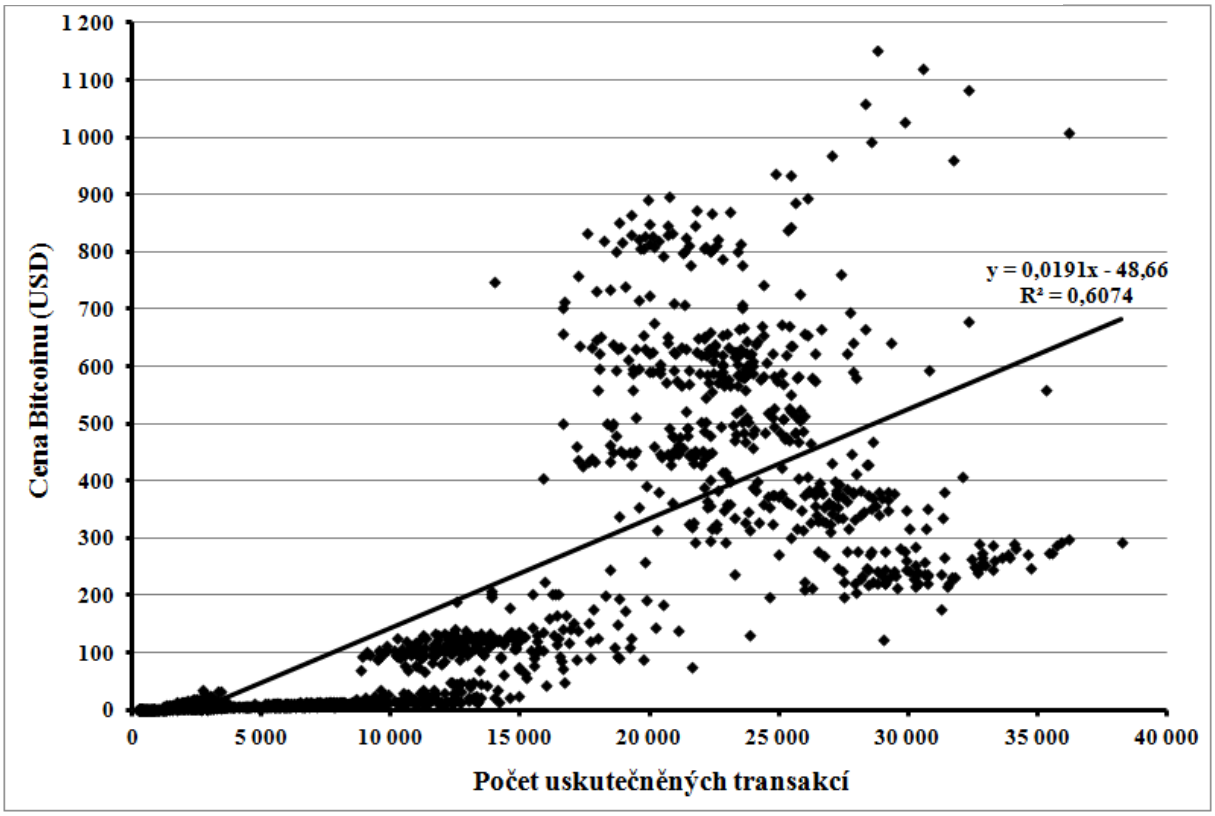
Zdroj: Blockchain (2015d,e), vlastní zpracování

Tento milník představuje v historii ceny Bitcoinu určitý zlom, který způsobil, že mnoho faktorů s dříve jasně identifikovanou úlohou v procesu utváření ceny Bitcoinu najednou ztratilo svůj význam, nebo se jejich role nějakým způsobem změnila. To dokládá třeba vzájemný vztah počtu uskutečněných transakcí a ceny Bitcoinu v USD, který obdobně

zkoumali např. Buchholz, Delaney, Warren, a Parker (2012). Lze tvrdit, že množství provedených transakcí bylo do konce roku 2013 hlavním hybatelem zvyšující se poptávky po Bitcoinu. Neboť jak znázorňuje graf 4.1, do tohoto zlomového období platilo, že čím více se zvyšoval počet uskutečněných transakcí, tím rostla i cena Bitcoinu. Od počátku roku 2014 však v tomto trendu nastává postupný obrat a dochází k rozcházení vývoje těchto dvou veličin.

Zajímavý je bližší pohled na sílu závislosti mezi těmito dvěma proměnnými. Pomocí Pearsonova korelačního koeficientu vypočtená hodnota $r_{xy} = 0{,}779$ vypovídá o silném stupni lineární závislosti. Protože jde o hodnotu větší než nula, dá se hovořit o pozitivní korelaci. Z grafu 4.1 je však patrné, že tento závěr není v souladu se znázorněným vývojem zejména v období posledních 12 měsíců. Prostřednictvím této metody rovněž nelze posoudit kauzalita závislosti mezi těmito dvěma proměnnými.

Graf 4.2 Regresní analýza ceny Bitcoinu a počtu uskutečněných transakcí



Zdroj: Blockchain (2015d,e), vlastní zpracování

Proto byla provedena regresní analýza (viz graf 4.2). Na rozdíl od pozdějších kapitol v této části práce je na tomto místě relativně snadné odhadnout, která proměnná je závislá (cena Bitcoinu v USD) a která nezávislá (počet uskutečněných transakcí). Použití této metody

je proto vhodné. Jak ukazuje graf 4.2, potvrdilo se výše uvedené – závislost ceny Bitcoinu při větších objemech provedených transakcí, typických hlavně pro období posledních 12 měsíců, je značně nepravidelná. Tomu ostatně odpovídá i vypočtená hodnota koeficientu determinace $R^2 = 0{,}607$, která znamená, že pouze přibližně 60,7% variability ceny Bitcoinu lze vysvětlit variabilitou počtu uskutečněných transakcí. Součástí grafu je i regresní přímka tvořená rovnicí $y = 0{,}0191x - 48{,}66$, která vypovídá o tom, že cena Bitcoinu přibližně odpovídá 0,02 násobku počtu uskutečněných transakcí sníženému o 48,66. Aplikovatelnost tohoto vztahu je však s ohledem na výše zmíněné podstatně omezená.

Oba grafy byly vytvořeny z dat poskytnutých portálem Blockchain.info za období od 17. srpna 2010 do 27. března 2015. Pro cenu Bitcoinu byla proto použita průměrná denní hodnota 1 bitcoinu v USD, za kterou se měna obchodovala na největších online burzách ve sledovaném období. Za ukazatel počtu uskutečněných transakcí byl zvolen celkový počet transakcí za každý den stejného období očištěný od transakcí, které byly součástí řetězců o délce více než 10 transakcí. Důvodem je skutečnost, že tyto dlouhé řetězce transakcí mohou kromě jiného znamenat snahu o umělé „nafukování“ počtu transakcí, nebo v horším případě pokusy o praní špinavých peněz. Například Gorale (2015) uvádí, že v roce 2014 vzrostl celkový objem Bitcoin transakcí o 45,5%, z čehož prý až polovinu mohly tvořit falešné transakční řetězce.

Bylo možné získat i starší data (doslova od okamžiku vytěžení prvního bitcoinu) avšak cena Bitcoinu je veličinou, která začala nabývat nenulových hodnot až právě v polovině srpna 2010, přičemž počet uskutečněných transakcí se do tohoto data držel na nízké a stabilní úrovni. Toto rané období Bitcoinu tedy nebylo zahrnuto pro lepší přehlednost grafů a za účelem menšího zkreslení výsledků regresní a korelační analýzy.

4.1 Faktory ovlivňující cenu Bitcoinu

Jak již bylo uvedeno ke konci podkapitoly 3.1.4, jednou z překážek bránící Bitcoinu v jeho masovém rozšíření je jeho nestabilní cena, která jej omezuje ve funkci uchovatele hodnoty. Toto kolísání je způsobeno tím, že Bitcoin jako digitální měna stejně jako klasické národní měny není ničím kryta v tom smyslu, že neexistuje nic (jako třeba zlato či jiný drahý kov) za co by se daly v pevně daném poměru směnit. Stejně jako třeba u dolaru zde není žádný obsah zlata či jiného drahého kovu v jednotce měny jako v dobách oběhu plnohodnotných mincí. V případě bitcoinu, jak bylo uvedeno v kapitole 3.4, dokonce ani fyzicky či digitálně neexistuje nic, na co by se dalo poukázat a říct o tom „tohle je bitcoin“.

Proč tedy klasické „konvenční“ měny mají relativně stálou hodnotu, kdežto u Bitcoinu dochází a hlavně v nedávné minulosti docházelo k výrazným výkyvům? Nápovědu je možné najít v první části této práce v kapitole 2.1, kde Jurečka a kol. (2010, s. 45) o penězích s prakticky nulovou vnitřní hodnotou tvrdí, že *„hodnota těchto peněz je založena na důvěře, že budou přijaty jako kupní a platební prostředek jinými subjekty společnosti.“* Protože ke vzniku Bitcoinu došlo teprve v relativně nedávné době, nebylo ještě dosaženo stavu, ve kterém by všechny subjekty v dané ekonomice přijímaly Bitcoin jako platební prostředek za zboží a služby. Jak uvádí Ciaian, Rajčániová a Kancs (2014), Bitcoin se nachází ve fázi budování podílu na trhu prostřednictvím zvyšování kredibility u potenciálních uživatelů. Vztah mezi akceptací Bitcoinu ekonomickými subjekty a volatilitou ceny Bitcoinu se ve své podstatě dá přirovnat vztahu v tradiční hádance o slepici a vejci. Zjednodušeně lze říct, že ustálí-li se cena Bitcoinu, více lidí jej začne používat, ale aby se cena Bitcoinu ustálila, je třeba, aby jej používalo více lidí.

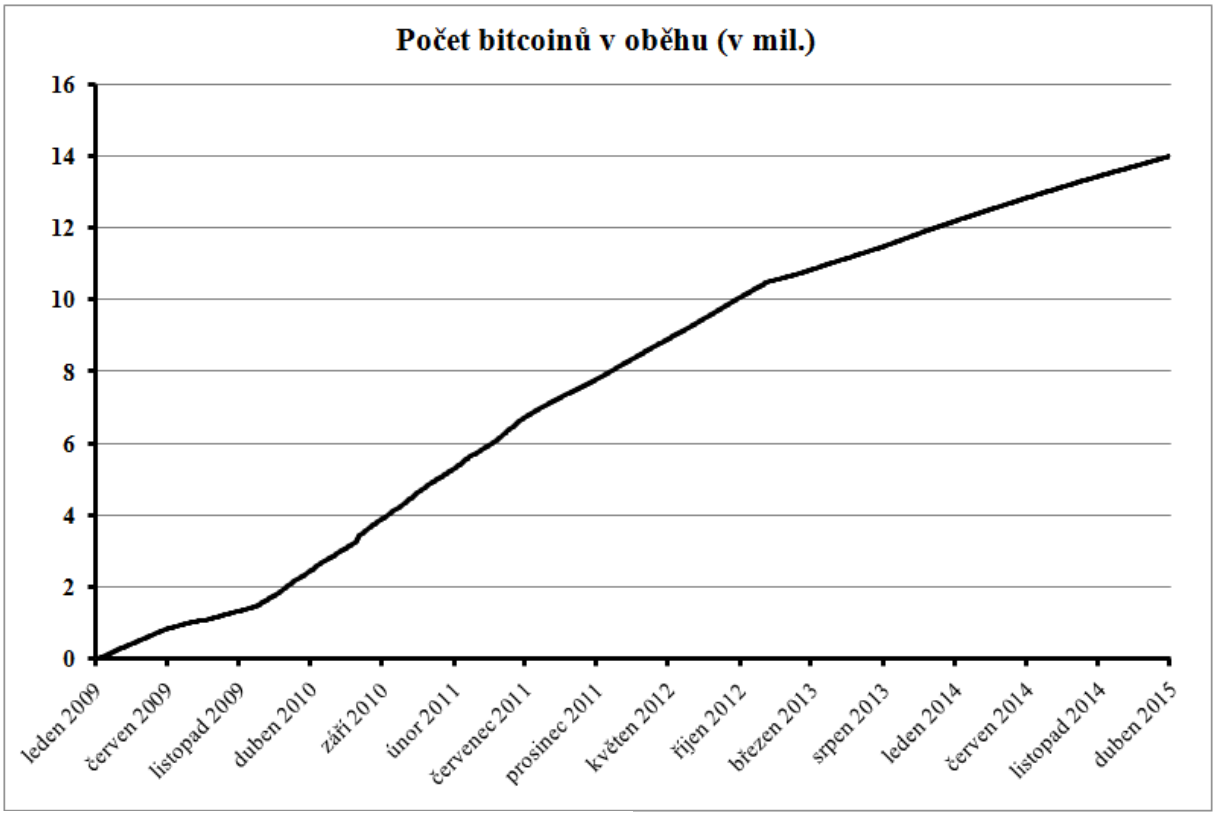
Ciaian, Rajčániová a Kancs (2014) považují za důležitý faktor také vliv médií. Ten může být na jednu stranu pozitivní v tom smyslu, že pomáhá vzbuzovat pozornost nových investorů a uživatelů. Zvyšuje-li se povědomí o Bitcoinu, roste i poptávka, čímž za jinak nezměněných okolností dochází k růstu ceny. Na druhou stranu, informují-li média např. o kybernetických útocích, k nimž je Bitcoin jako čistě digitální měna přirozeně náchylnější, může to stávající investory motivovat k prodeji svých bitcoinů a poohlížení se po jiných investičních příležitostech. Hromadné prodeje na burzách obecně vedou k poklesu ceny daného aktiva.

4.2 Nabídka

Jedním z hlavních determinantů výsledné ceny je nabídka, která má v případě Bitcoinu určité zvláštní charakteristiky. Jedním ze znaků nabídky Bitcoinu je její předem stanovený a v čase se zpomalující růst. Nové bitcoiny jsou do oběhu uvolňovány přibližně každých 10 minut s tím, jak dochází k připojování nových bloků transakcí do block chainu a vyplácení odměn těžařům, kterým se to podařilo (viz kapitola 3.3). Tato odměna původně činila 50 bitcoinů, v současné době je snížená na polovinu a předpokládá se, že k dalšímu snížení (na 12,5 bitcoinu) dojde někdy v polovině roku 2016. Bitcoin software je navržen tak, že se tento proces snižování odměny na polovinu opakuje každé 4 roky a uvolňování nových bitcoinů má přestat až po dosažení 21 milionů kusů v oběhu (v současnosti je v oběhu něco málo přes 14 milionů bitcoinů – viz graf 4.3), k čemuž by mělo dojít někdy mezi lety 2110 a

2140. Dá se tedy předpokládat, že se zpomalujícím se tempem emise bitcoinů a nakonec i jejím ukončením v určitém bodě v budoucnu poroste jejich vzácnost a tím i cena. To může být dobrou iniciativou k tomu, aby více lidí začalo používat Bitcoin, protože tím vzniká určitá forma záruky hodnoty v budoucnu.

Graf 4.3 Současná nabídka bitcoinů



Zdroj: Blockchain (2015c), vlastní zpracování

Takovýto charakter nabídky s sebou nese i aspekt deflace, na který v literatuře existují rozporuplné názory. Například Varoufakis (2013) považuje deflaci za jednu ze základních a nepřekonatelných vad Bitcoinu. Poukazuje na to, že kdyby se Bitcoin prosadil jako světová měna, rapidně by na trhu přibývalo zboží a služeb obchodovatelných v bitcoinech, čemuž by pomalu se zvyšující nabídka neměla šanci se přizpůsobit. Tím by docházelo k poklesu množství dostupných bitcoinů na jednu jednotku zboží a služeb, což by způsobilo pokles cenové hladiny – deflaci. Očekávaný pokles cen by motivoval ekonomické subjekty k odkládání plateb do budoucna, čímž by klesala agregátní poptávka. Navíc za předpokladu, že existuje určitý časový interval mezi nákupem výrobních faktorů a uvedením finálního produktu na trh, nakupovaly by firmy své vstupy při vyšší cenové hladině, než při jaké by prodávaly své výstupy, čímž by docházelo k poklesu jejich zisků. S klesajícími zisky

je spojen snižující se objem investic, propouštění či úplné zastavení výroby. Na druhou stranu Šíma (2002) považuje deflaci za přirozený stav dynamicky se rozvíjejícího hospodářství. Při rostoucí produkci statků a neměnné peněžní zásobě (kterou by v tomto případě představovala nabídka bitcoinů) jsou výrobci nuceni mezi sebou čím dál více soutěžit o každou jednotku peněz. To způsobí růst kupní síly peněz, zvýší se jejich hodnota, čímž dojde k poklesu cen. Dojde také k omezení plýtvání, což vytvoří podmínky pro další růst.

4.3 Poptávka

Buchholz, Delaney, Warren, a Parker (2012) poznamenávají, že nabídka je exogenní, tudíž nemá žádný vztah s poptávkou ani cenou Bitcoinu. A protože nabídka v případě Bitcoinu nijak nereaguje na změny v ceně, musí být její fluktuace způsobena změnami v poptávce.

V úvodu této části práce bylo hovořeno o vlivu počtu uskutečněných transakcí na cenu Bitcoinu. To bylo zpočátku považováno za hlavního hybatele zvyšující se poptávky po Bitcoinu, protože se potvrdilo, že počet uskutečněných transakcí skutečně pozitivně koreloval s cenou Bitcoinu zejména v období prvních let existence Bitcoinu. To se dá vysvětlit tím, že povědomí veřejnosti o Bitcoinu bylo v té době ještě velmi nízké a převážnou část uživatelské základny Bitcoinu tvořili spíše technologičtí nadšenci, inovátoři a lidé, kteří přestali z nějakého důvodu důvěřovat finančním institucím. Ukázalo se také, že po prosinci roku 2013 už změny v počtu uskutečněných transakcí nemohou být považovány za hlavní sílu působící v procesu utváření ceny Bitcoinu především kvůli událostem z října a listopadu 2013 (viz úvod této části práce). Autor práce proto předpokládá, že tento obrat ve vývoji byl způsoben tím, že v důsledku zvýšené publicity se tehdy v ekosystému Bitcoinu výrazně zvětšil segment uživatelů tvořený zejména investory, spekulanty a obecně osobami, kteří „používají“ Bitcoin za účelem zisku. Tento typ osob je charakteristický tím, že hromadí velká množství bitcoinů s úmyslem prodeje v budoucnu.

Jinými slovy, v další části této práce bude tato skupina investorů, spekulantů a osob s podobnými zájmy (dále jen „investoři“) považována za hlavního činitele způsobujícího výkyvy v poptávce po Bitcoinu a potažmo i v ceně Bitcoinu. Bude využito toho, že tyto osoby považují Bitcoin za příležitost jak diverzifikovat své investiční portfolio, navzdory tomu že primárním účelem Bitcoinu je sloužit jako digitální měna a zprostředkovávat platby za zboží a služby bez participace třetí strany (jako je stát, banka či korporace). Prvním předpokladem je, že tyto osoby mění svoje investiční chování v závislosti na vývoji některých finančních a

makroekonomických indikátorů. Například procházejí-li finanční trhy příznivým obdobím, rostou investorům zisky ze standardních finančních investičních instrumentů a tyto zisky jim poskytují prostředky k dalším investicím, třeba právě do Bitcoinu. Nebo jiný příklad, klesá-li cena nějakého investičního aktiva, dává to investorům podnět k hledání jiných investičních příležitostí, Bitcoin představující jednu z nich. Druhým předpokladem je, že neexistují náklady na získání informací o Bitcoinu a náklady na pochopení a naučení se zacházení s touto relativně novou technologií, jež by jinak představovaly překážku pro některé investory.

Jak ale vybrat vhodné finanční a makroekonomické ukazatele tak, aby byly dostatečně reprezentativní a relevantní? Na tomto místě je příhodné upozornit na závěry, ke kterým došel van Wijk (2013). Objevil, že existuje statisticky významný vztah mezi cenou Bitcoinu a třemi dalšími veličinami – hodnotou indexu Dow Jones, hodnotou směnného kurzu dolaru a eura a cenou barelu ropy. Tyto veličiny proto budou předmětem empirické analýzy v následujících podkapitolách. Bude přitom využito metody korelace, která bude spočívat ve výpočtu Pearsonova korelačního koeficientu mezi dvěma proměnnými (jednou z nich bude vždy cena Bitcoinu). Proměnné budou představovat vždy dvě odlišné časové řady daných veličin. První časová řada vznikne prodloužením původního sledovaného období a její analýza poslouží k ověření, zda dosavadní závěry, ke kterým bylo dospěno v literatuře, platí i v delším časovém intervalu. Druhá časová řada se bude týkat výhradně období od „velkého cenového skoku“, který Bitcoin zaznamenal ke konci roku 2013 až po současnost. Toto kratší sledované období je z důvodů uvedených výše v této kapitole zkoumáno samostatně v podkapitole 4.3.5.

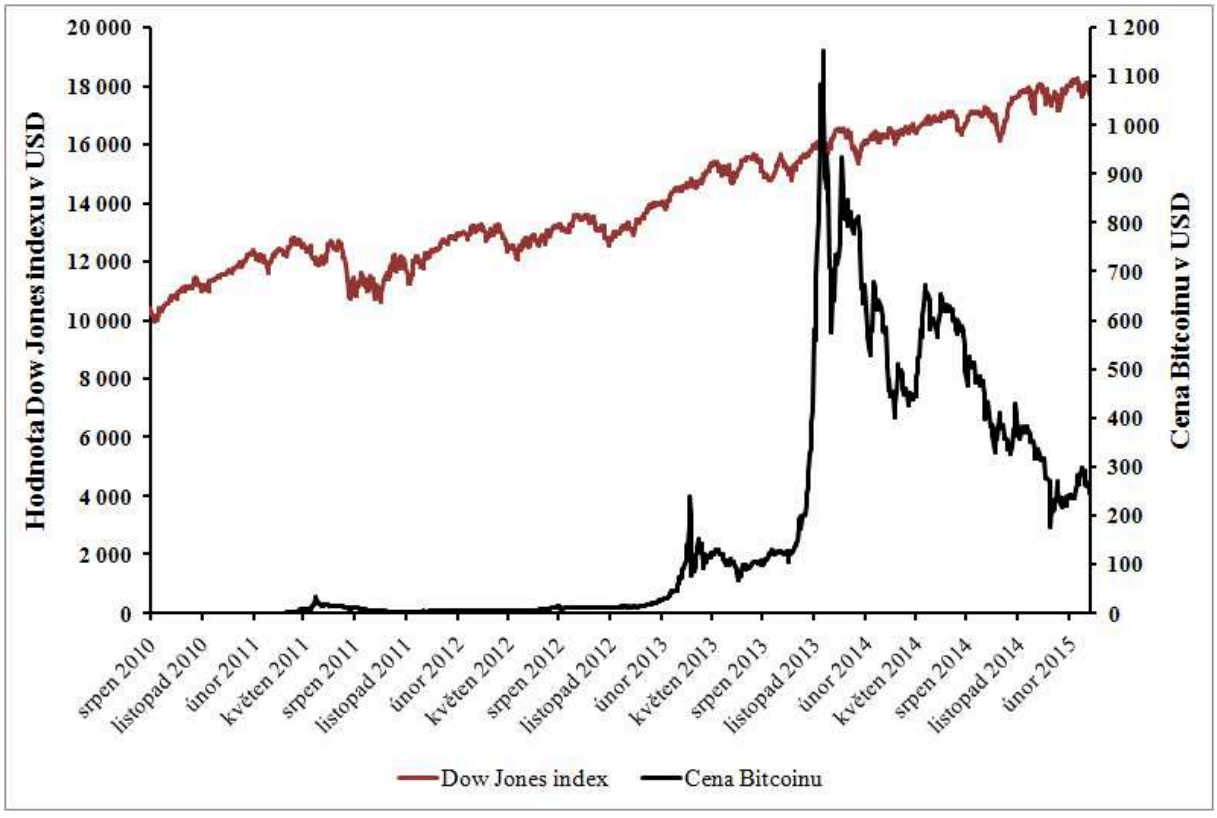
4.3.1 Dow Jones index

Někdy také označovaný jako Dow Jones Industrial Average je burzovní index sestavovaný již od roku 1896, jedná se tedy o jeden z nejstarších burzovních indexů vůbec. Technicky jde o cenově vážený průměr akcií 30 největších amerických společností obchodovaných na newyorských burzách NYSE a NASDAQ. Bývá proto považován za jeden z hlavních ukazatelů výkonnosti ekonomiky Spojených států. Van Wijk (2013) došel k závěru, že cena Bitcoinu pozitivně koreluje s hodnotou Dow Jones indexu v krátkém i dlouhém období. Z toho odvodil, že příznivý vývoj americké ekonomiky má pozitivní vliv na cenu Bitcoinu. Při výpočtech vycházel z denních dat ceny Bitcoinu v USD získaných z tehdy největší online burzy obchodující s Bitcoinem, Mt. Gox, a hodnoty Dow Jones indexu v USD

za období od 19. července 2010 do 13. června 2013 s výjimkou víkendů, státních svátků a jiných dnů kdy se na burzách neobchodovalo.

V této podkapitole bude proměnnou cena Bitcoinu představovat časová řada tvořená denními daty pro cenu Bitcoinu v amerických dolarech za období od 17. srpna 2010 (dne, kdy cena Bitcoinu zaznamenaná portálem Blockchain.info poprvé nabyla nenulovou hodnotu) do 27. března 2015 (přibližného období zpracovávání této části práce). Proměnná hodnota Dow Jones indexu je tvořená časovou řadou sestavenou z denních dat pro hodnotu indexu Dow Jones Industrial Average v amerických dolarech za stejné období. U ceny Bitcoinu byly z dat vypuštěny záznamy za víkendy, státní svátky a jiné dny, kdy se neobchoduje na burze proto, aby byla zachována stejná frekvence a počet záznamů jako u Dow Jones indexu. Použití takto upravených denních dat bylo upřednostněno před použitím průměrných týdenních dat proto, aby nedocházelo ke zbytečně velkému zkreslení výsledků. Oba soubory dat tedy obsahují celkem 1160 pozorování. Data pro cenu Bitcoinu pocházejí z databáze portálu Blockchain.info, data pro hodnotu Dow Jones indexu jsou ze statistické databáze brazilské centrální banky. Oba soubory dat byly staženy z portálu Quandl.com a zpracovány v programu MS Office Excel 2007.

Graf 4.4 Vývoj hodnoty Dow Jones indexu a ceny Bitcoinu ve sledovaném období



Zdroj: Blockchain (2015d), Quandl.com (2015), vlastní zpracování

Graf 4.4 znázorňuje vývoj obou veličin ve sledovaném období. Hodnota Pearsonova koeficientu korelace zaokrouhlená na 3 desetinná místa vyšla $r_{xy} = 0{,}756$, lze tedy potvrdit silný stupeň lineární závislosti. Protože je výsledná hodnota kladná, jde o pozitivní korelaci. Dá se proto předpokládat, že roste-li hodnota jedné proměnné, nastane růst i u druhé a naopak. V rámci této metody ale není určeno, která z proměnných je závislá a která nezávislá. Pokud by bylo vycházeno z odhadu, že cena Bitcoinu je závislá na hodnotě Dow Jones indexu, potvrdila by se i interpretace uvedená na začátku této podkapitoly, tedy že dobře se vyvíjející americká ekonomika má příznivý vliv na cenu Bitcoinu. Výsledky by se daly vysvětlit i tak, že rostoucí hodnota indexu Dow Jones signalizuje rostoucí zisky akcionářů největších amerických společností (ať už v podobě růstu ceny akcií nebo vyplácení vyšších dividend) a vzbuzuje mezi nimi optimizmus. To investory vede k vyhledávání nových investičních příležitostí, přičemž jednou z nich může být právě Bitcoin. Zvyšuje-li se zájem o investice do Bitcoinu, povede to ceteris paribus k růstu ceny Bitcoinu.

4.3.2 Směnný kurz USD/EUR

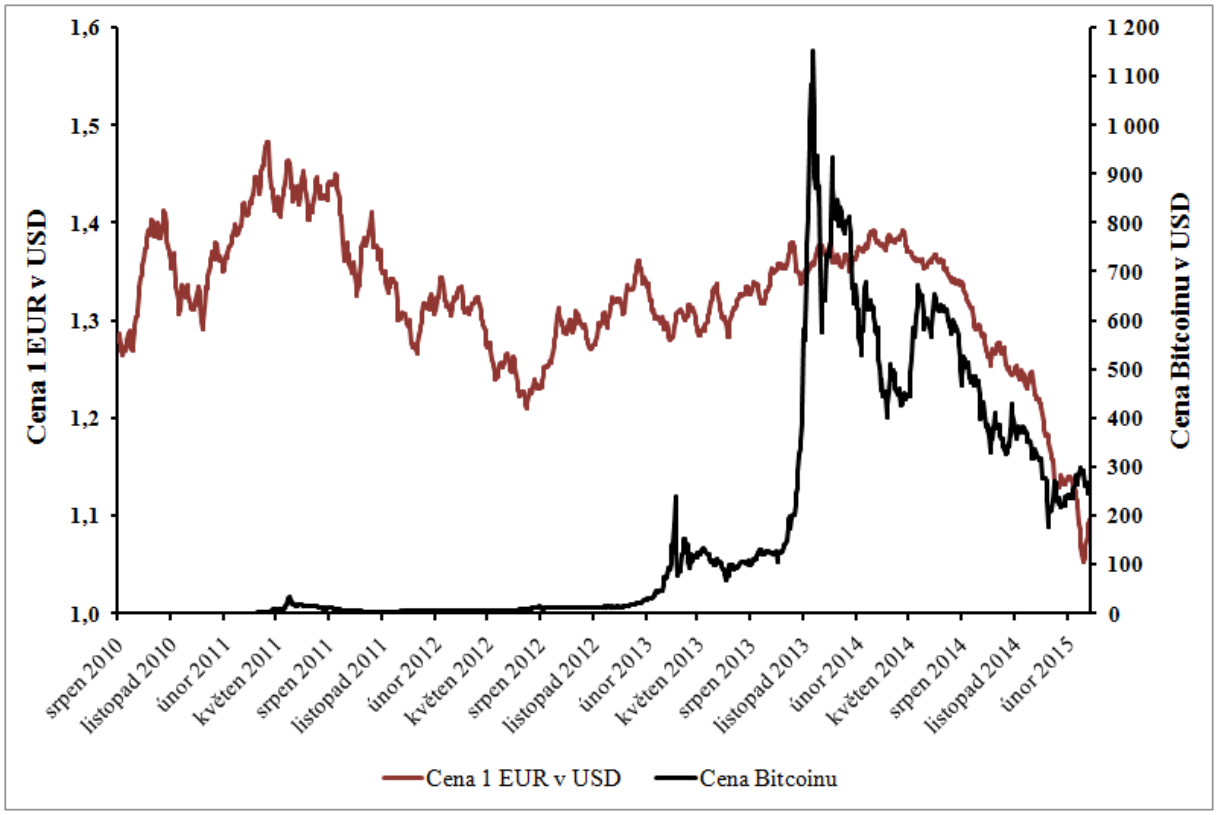
Dalším indikátorem, u kterého byl objeven vztah s cenou Bitcoinu je směnný kurz USD/EUR. Tento kurz představuje cenu 1 jednotky eura vyjádřenou v jednotkách amerického dolaru. Van Wijk (2013) konkrétně použil tento kurz v nepřímé kotaci a odhalil negativní korelaci s cenou Bitcoinu v USD v dlouhém období. Interpretoval to tím, že apreciuje-li dolar vůči euru, měla by americká měna s velkou pravděpodobností apreciovat rovněž i vůči Bitcoinu. V důsledku toho by se měl snižovat počet jednotek dolaru nutných k nákupu 1 jednotky Bitcoinu, čímž logicky dochází k poklesu ceny Bitcoinu v dolarech.

Stejně jako při testování vlivu Dow Jones indexu na cenu Bitcoinu bude původní sledované období (od 19. 7. 2010 do 13. 6. 2013) změněno, resp. prodlouženo na dobu mezi daty 17. srpna 2010 a 27. března 2015. V tomto případě chybí v datech o hodnotě směnného kurzu USD/EUR oproti souboru dat pro cenu Bitcoinu v USD pouze údaje za víkendy. Po upravení dat patřičným způsobem je tak pro výpočty k dispozici 1204 pozorování. Proměnnou cena Bitcoinu reprezentuje stejný soubor dat jako v minulé podkapitole, soubor dat pro hodnotu směnného kurzu USD/EUR, stažený z portálu Quandl.com, pochází z databáze Wiki Exchange Rates. Tato databáze je vhodným zdrojem, protože získává záznamy o hodnotě směnných kurzů sloučením hodnot z několika různých zdrojů, např. z údajů burz, centrálních bank aj. Směnný kurz je vyjádřen v přímé kotaci, vyjadřuje tedy cenu 1 jednotky eura v jednotkách amerického dolaru. Tento způsob byl upřednostněn před nepřímou kotací, protože se jedná o rozšířenější a obvyklejší způsob zápisu. Pro potvrzení závěru, ke kterému došel van

Wijk (2013), bude proto potřeba, aby výsledkem korelační analýzy byla pozitivní korelace mezi danými proměnnými. Sníží-li se totiž hodnota proměnné cena 1 EUR v USD, měla by se snížit i cena Bitcoinu v USD, neboť tím dochází k apreciaci americké měny.

Vývoj uvedených veličin ve sledovaném období je znázorněn v grafu 4.5. Hodnota Pearsonova korelačního koeficientu zaokrouhlená na 3 desetinná místa je $r_{xy} = 0{,}013$, nejde tedy o statisticky významnou závislost. Hodnota blízká nule signalizuje, že zkoumané veličiny se v čase vyvíjejí nezávisle na sobě, a že mezi nimi neexistuje lineární závislost. V tomto prodlouženém časovém intervalu tedy nelze potvrdit premisu o pozitivní korelaci mezi cenou Bitcoinu a hodnotou směnného kurzu USD/EUR.

Graf 4.5 Vývoj hodnoty směnného kurzu USD/EUR (ceny 1 EUR v USD) a ceny Bitcoinu ve sledovaném období



Zdroj: Blockchain (2015d), Quandl.com (2015), vlastní zpracování

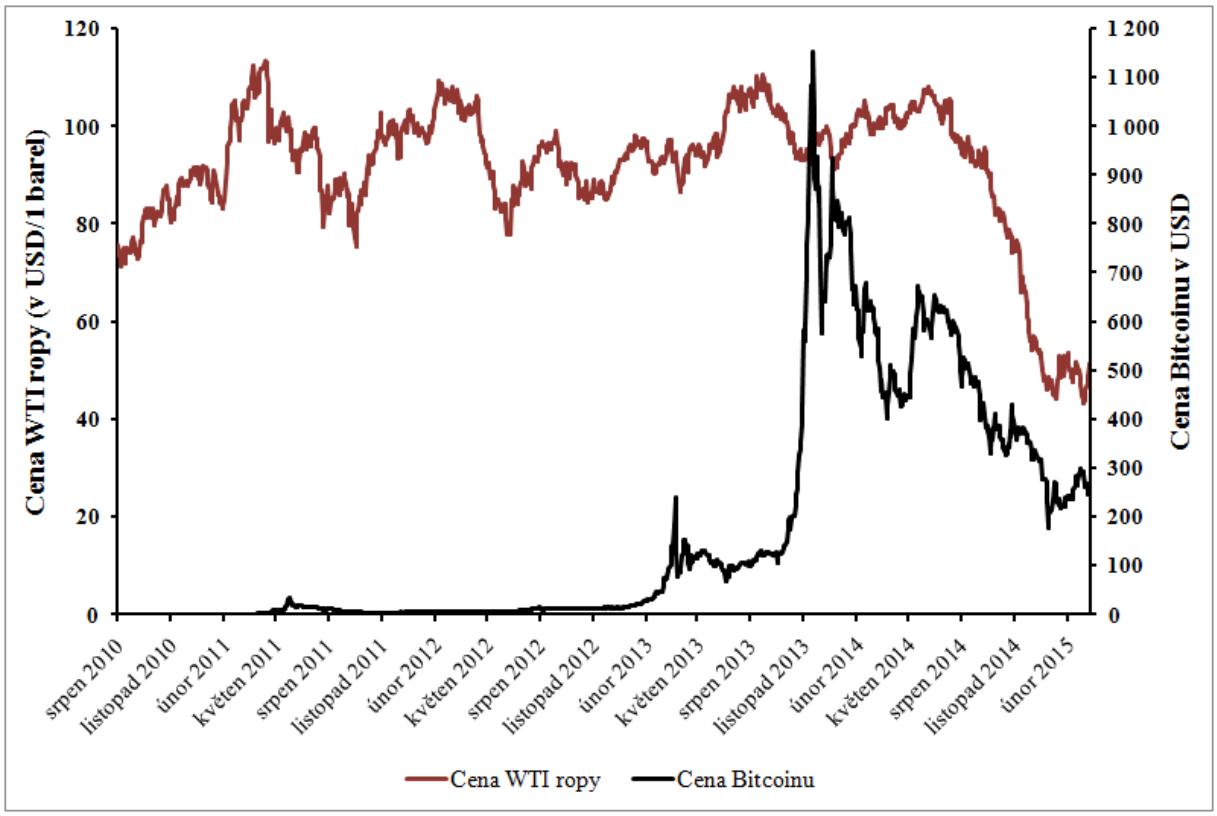
4.3.3 Cena ropy

Posledním ukazatelem, u kterého byla objevena určitá spojitost s vývojem ceny Bitcoinu, je cena ropy vyjádřená v dolarech za 1 barel WTI ropy. Zkratka WTI znamená West Texas Intermediate a označuje specifický druh ropy původem z Texasu a jižní Oklahomy. Cena tohoto druhu ropy se používá jako referenční hodnota v oceňování ostatních druhů ropy těžených v Severní Americe. Mezi jiné konkurenční druhy ropy patří např. směsná ropa Brent, zahrnující 15 druhů ropy z nalezišť v Severním moři. Podle závěrů, ke kterým van Wijk (2013) došel, existuje mezi vývojem ceny barelu WTI ropy a ceny Bitcoinu v dlouhém období negativní korelace. Podle jeho interpretace zdražení WTI ropy vyvolá pokles reálných zůstatků spotřebitelů, čímž dojde k poklesu objemu prostředků použitelných na nákup jiných statků, např. Bitcoinu. Dojde tak k poklesu celkové poptávky po Bitcoinu což vyvolá pokles jeho ceny.

Testování tohoto vztahu bude provedeno stejně jako v předchozích podkapitolách, tj. znázorněním vývoje zkoumaných proměnných v čase v grafu a výpočtem Pearsonova korelačního koeficientu. Bude rovněž dodrženo stejné sledované období. Proměnnou cena WTI ropy představuje časová řada tvořená denními daty pro cenu 1 barelu WTI ropy v amerických dolarech, proměnnou cena Bitcoinu tvoří stejná časová řada jako v předchozích podkapitolách. Soubor dat pro cenu WTI ropy pochází z databáze výzkumného oddělení St. Louiské federální rezervní banky a byl stažen z portálu Quandl.com. Kompenzace absence záznamů za víkendy, státní svátky a jiné dny, kdy se s komoditou na burze neobchodovalo, v datech pro cenu WTI ropy byla provedena stejným způsobem jako v podkapitole 4.3.1. Pro výpočty je tak k dispozici 1166 pozorování.

Vývoj ceny WTI ropy a ceny Bitcoinu ve sledovaném období je znázorněn v grafu 4.6, není z něj však patrné, zda mezi těmito dvěma veličinami existuje nějaký vztah. To dokládá i vypočtená hodnota Pearsonova korelačního koeficientu zaokrouhlená na 3 desetinná místa, $r_{xy} = 0{,}035$. Hodnota se blíží nule, lze tedy celkem s jistotou předpokládat, že mezi danými proměnnými neexistuje žádná statisticky významná lineární závislost. Pro cenu Bitcoinu to znamená, že její hodnota se v prodlouženém období vyvíjí nezávisle na ceně WTI ropy. Nelze tak potvrdit, že by zde existoval nějaký vzájemný vztah.

Graf 4.6 Vývoj ceny WTI ropy (v USD/1 barel) a ceny Bitcoinu ve sled. období



Zdroj: Blockchain (2015d), Quandl.com (2015), vlastní zpracování

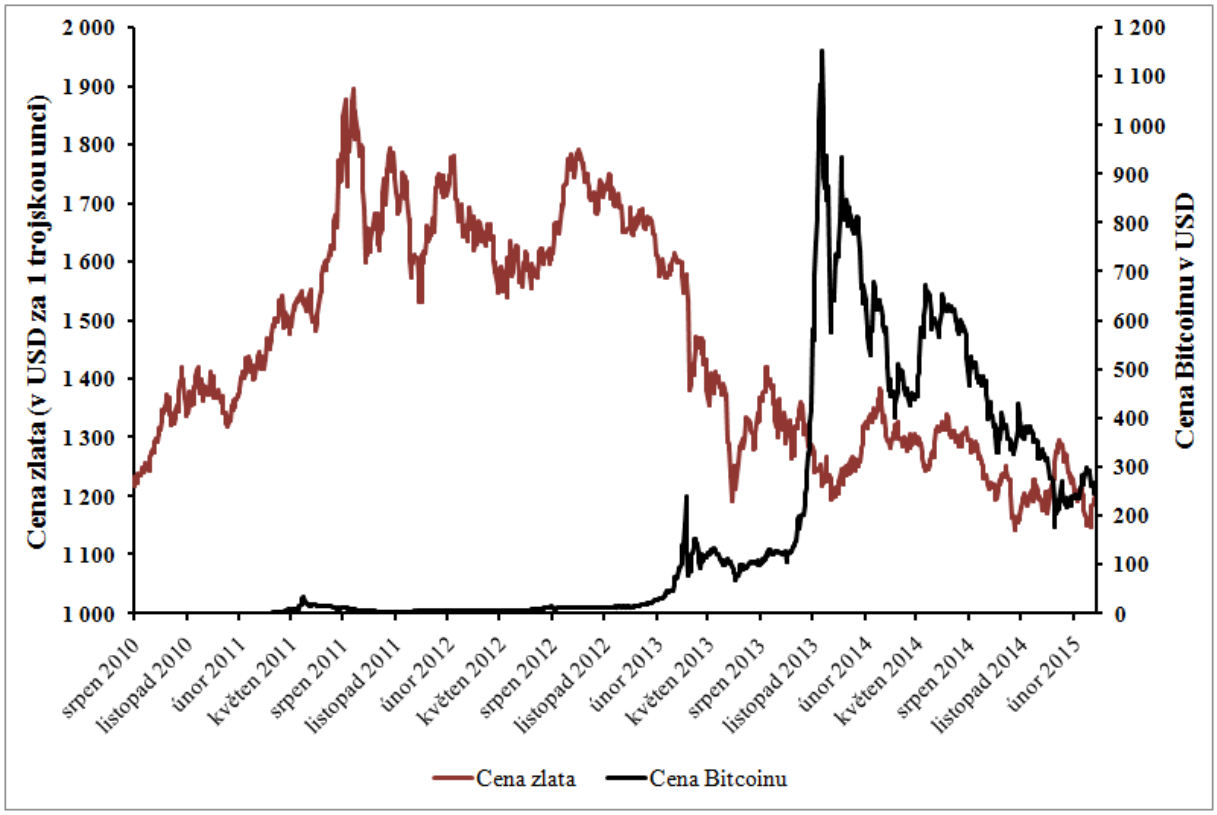
4.3.4 Cena zlata

Posledním faktorem, jehož souvislost s vývojem ceny Bitcoinu bude zkoumána v této práci je cena zlata. Proč zrovna zlato? Ač se to na první pohled nemusí zdát až tak patrné, Bitcoin a zlato mají mnoho společných charakteristických znaků. Varoufakis (2013) dokonce uvádí, že tvůrce Bitcoinu, Satoshi Nakamoto, se snažil ze všech sil, aby jeho výtvor co nejvíce napodoboval zlato. Stejně jako zlato, u něhož se předpokládá, že pod zemským povrchem existuje pouze v omezeném množství, tak i počet Bitcoinů je pevně omezen (viz kapitola 4.2). A stejně jako v případě zlata existují 2 způsoby jak získat Bitcoin – koupit jej za peníze, nebo jej vytěžit (viz kapitola 3.3). Co se týče těžby, i Bitcoin zažil ve svých počátcích obdobu zlaté horečky 19. století, kdy náročnost těžby byla ještě relativně nízká. S tím jak byl ale algoritmus Bitcoinu nastaven a čím dál více bitcoinů bylo vytěženo, rostla exponenciálně i náročnost těžby. A stejně jako zlato, i Bitcoin se v současné době vyplatí těžit jen „velkým“ těžařům, kteří využívají úspor z rozsahu. Poslední aspekt, ve kterém jsou si tyto dvě komodity podobné, jsou funkce, které plní, plnily, nebo mají plnit. Zlato plnilo funkci prostředku směny v dobách komoditních a později plnohodnotných peněz (viz kapitola 2.1) a i v současné době

dokáže plnit funkci uchovatele hodnoty. Bitcoin umí plnit funkci prostředku směny a má i předpoklady k tomu, aby plnil i funkci uchovatele hodnoty.

Na základě uvedených podobností se autor práce domnívá, že by mezi cenou zlata a cenou Bitcoinu mohl existovat určitý vztah, neboť se jedná víceméně o vzájemné komplementy. Hypotéza je taková, že poroste-li cena jednoho aktiva v důsledku rostoucí poptávky po tomto aktivu, zvýší se i zájem investorů o druhé aktivum, a tím i jeho cena. Pro ověření této hypotézy bude použita stejná metoda jako ve třech předchozích podkapitolách. V období od 17. 8. 2010 do 27. 3. 2015 bude prostřednictvím grafu sledován vývoj ceny Bitcoinu a ceny zlata, kterou bude představovat cena 1 trojské unce zlata vyjádřená v amerických dolarech. Soubor dat pro tuto veličinu pochází z databáze organizace usilující o rozvoj trhu se zlatem, The World Gold Council. Z dat pro cenu Bitcoinu byly vypuštěny záznamy za víkendy, aby byla zachována časová kompatibilita s daty pro cenu zlata. Oba soubory dat byly staženy z portálu Quandl.com a obsahují každý celkem 1205 pozorování.

Graf 4.7 Vývoj ceny zlata (v USD za 1 trojskou unci) a ceny Bitcoinu ve sledovaném



Zdroj: Blockchain (2015d), Quandl.com (2015), vlastní zpracování

Graf 4.7 zobrazuje vývoj obou veličin ve sledovaném (dlouhém) období. V některých částech (zejména během roku 2013) je patrné, že mezi hodnotami proměnných

dochází k opačnému vývoji. Pearsonův korelační koeficient má v tomto případě hodnotu r_{xy} = -0,633, což vypovídá o statisticky významné lineární závislosti. Hodnota koeficientu vyšla záporně, jedná se tedy o negativní korelaci. Není proto možné potvrdit hypotézu o současném růstu cen obou veličin. Výsledky spíše naznačují, že se jedná o vzájemné substituty, neboť růst ceny jednoho aktiva znamená pokles ceny druhého aktiva a naopak. Interpretovat by se to dalo tím, že dojde-li např. k poklesu ceny Bitcoinu, část investorů se rozhodne zhodnotit své prostředky jiným způsobem, např. investicí do zlata. Tím dojde ke zvýšení poptávky po zlatě a za jinak nezměněných okolností i ke zvýšení jeho ceny.

4.3.5 Období „po velkém cenovém skoku“

V této podkapitole bude samostatně zkoumán vývoj veličin (resp. proměnných) uvedených v podkapitolách 4.3.1 až 4.3.4 vůči ceně Bitcoinu v období od přelomu listopadu a prosince 2013, kdy došlo k razantnímu růstu ceny Bitcoinu, až po současnost. Toto období bude technicky vymezeno od 2. prosince 2013[21] do 27. března 2015 (přibližného období zpracovávání této části práce). Pro výpočty budou sloužit stejné datové soubory pocházející ze stejných zdrojů jako v předchozích podkapitolách. Použity budou i stejné metody. V důsledku zkrácení sledovaného období je pro hodnotu Dow Jones indexu k dispozici 330 pozorování, pro cenu ropy 335 pozorování a pro hodnotu směnného kurzu USD/EUR a cenu zlata shodně 345 pozorování. Výpočty koeficientů byly prováděny v programu MS Office Excel 2007.

Hodnota indexu Dow Jones se v tomto kratším sledovaném období vyvíjí ve vztahu k ceně Bitcoinu naprosto opačným směrem (ve srovnání s vývojem v prodlouženém období). Podobný jev bylo možné pozorovat u vztahu mezi množstvím provedených transakcí a cenou Bitcoinu. Výsledná hodnota Pearsonova korelačního koeficientu pro tento časový interval zaokrouhlená na 3 desetinná místa vychází r_{xy} = -0,771, což sice stejně jako v prvním případě svědčí o silném stupni lineární závislosti, avšak zde se jedná o korelaci negativní. To znamená, že při poklesu jedné proměnné dochází k růstu druhé proměnné a naopak. Dá se tedy s jistotou říci, že po období „velkého cenového skoku“ Bitcoinu ke konci roku 2013 již neplatí tvrzení, že pozitivní vývoj hospodářství Spojených států pozitivně koreluje s vývojem ceny Bitcoinu.

V případě směnného kurzu USD/EUR nebyl v prodlouženém období objeven statisticky významný vztah k ceně Bitcoinu (viz podkapitola 4.3.2). V období po „velkém

[21] Přesný přelom měsíce listopadu a prosince 2013 nelze použít, neboť datum 30. 11. 2013 a 1. 12. 2013 připadlo na sobotu a neděli. Pro tyto dny data z finančních trhů pro zkoumané veličiny z očividných důvodů neexistují.

cenovém skoku“ Bitcoinu je však situace odlišná. Pearsonův koeficient korelace má pro tento časový interval (2. 12. 2013 – 27. 3. 2015) hodnotu (zaokrouhlenou na 3 desetinná místa) r_{xy} = 0,777, což vypovídá o silném stupni lineární závislosti mezi proměnnou cena 1 EUR v USD a cena Bitcoinu. Kladná hodnota svědčí o pozitivní korelaci, dochází-li tedy k růstu jedné proměnné, roste i hodnota druhé a naopak. Klesala-li cena 1 jednotky eura v jednotkách amerického dolaru v tomto kratším sledovaném období tak skutečně docházelo i k poklesu ceny Bitcoinu v USD. Tím jak měna Spojených států apreciovala vůči euru, klesalo i množství jednotek této měny nutných ke koupi 1 bitcoinu, čímž docházelo k poklesu ceny Bitcoinu.

Podle výsledků v podkapitole 4.3.3 nebylo možné označit závislost mezi cenou ropy a cenou Bitcoinu v prodlouženém časovém intervalu za statisticky významnou. Naopak je tomu v kratším sledovaném období. Hodnota Pearsonova korelačního koeficientu zaokrouhlená na 3 desetinná místa vyšla r_{xy} = 0,741, jedná se tedy o silný stupeň lineární závislosti. Hodnota koeficientu je větší než nula, mezi proměnnými proto existuje pozitivní korelace. Lze tvrdit, že současně s poklesem hodnoty proměnné cena WTI ropy docházelo ve sledovaném období i k poklesu hodnoty proměnné cena Bitcoinu a naopak.

Cena zlata se v prodlouženém období vyvíjela v negativní korelaci s cenou Bitcoinu (viz podkapitola 4.3.4). V kratším sledovaném období je situace opačná. Hodnota Pearsonova korelačního koeficientu zaokrouhlená na 3 desetinná místa vyšla r_{xy} = 0,376, mezi proměnnými tedy existuje určitá slabá lineární závislost. Kladná hodnota svědčí o pozitivní korelaci, dochází-li tedy k růstu jedné proměnné, roste i hodnota druhé a naopak. Lze proto tvrdit, že po tom, co Bitcoin zaznamenal ke konci roku 2013 velký cenový nárůst, vykazovala cena Bitcoinu podobný trend jako cena zlata. V případě tohoto specifického období se tak do určité míry dá potvrdit původní hypotéza uvedená v podkapitole 4.3.4, tedy že jde vskutku o vzájemné komplementy.

Na základě dosažených výsledků se nabízí následující interpretace. Období od 2. prosince po současnost bylo charakteristické přetrvávajícím poklesem ceny Bitcoinu s občasnými korekcemi. Velká část investorů proto pravděpodobně prodala svoje bitcoiny způsobujíc další pokles a přesunula své prostředky jinam. Jednou z příležitostí jak zhodnotit svůj majetek nabízely akcie amerických podniků, jejichž rostoucí vývoj reprezentovala rostoucí hodnota Dow Jones indexu. To by mohlo vysvětlovat silný stupeň negativní korelace mezi cenou Bitcoinu a hodnotou Dow Jones indexu v daném období. V tomto časovém intervalu také došlo k výrazné apreciaci amerického dolaru zejména pak v období 2. poloviny roku 2014, což by mohlo vysvětlovat silný stupeň pozitivní korelace ceny Bitcoinu

s hodnotou směnného kurzu USD/EUR. Americká měna posilovala nejen vůči euru, ale i vůči Bitcoinu, čímž přispěla k poklesu jeho ceny. Je to velký rozdíl oproti prodlouženému období, ve kterém z velké části k výrazným výkyvům kurzu nedocházelo, což se podepsalo i na výsledcích (viz podkapitola 4.3.2). Nepravidelný vývoj ceny ropy v prodlouženém období (viz graf 4.6) nasvědčuje tomu, že pozitivní korelace s cenou Bitcoinu v období po „velkém cenovém skoku“ je spíše náhodná a spojitost mezi vývojem ceny ropy a cenou Bitcoinu lze označit celkově za nanejvýš pochybnou. Podobná je situace u ceny zlata, kde v 2. polovině prodlouženého období nastává zásadní změna ve vývoji, čímž dochází k rozcházení výsledků v kratším sledovaném časovém intervalu. V krátkém období se tak nepotvrdil vztah, který byl objeven mezi cenou zlata a cenou Bitcoinu v dlouhém období.

4.4 Dílčí shrnutí

Předmětem této části práce bylo zkoumání faktorů, které ovlivňují cenu Bitcoinu. Byla zde empiricky ověřena platnost teoretických i empirických poznatků uvedených v dostupné literatuře. Důvodem pro ověřování byla skutečnost, že většina autorů prováděla svoji analýzu před téměř dvěma roky, což v případě vysoce dynamického vývoje, kterým Bitcoin prošel a v současnosti stále prochází, představuje dávnou minulost. V kapitolách této části práce byly popsány hlavní faktory ovlivňující vývoj ceny Bitcoinu. Patří mezi ně nabídka, která je v případě Bitcoinu pevně stanovená, a poptávka, na níž působí další vlivy. Mezi vedlejší faktory patří např. nedostatečná akceptace Bitcoinu ekonomickými subjekty či vliv médií. Byl učiněn závěr, že největší vliv na vývoj ceny Bitcoinu mají výkyvy v poptávce po Bitcoinu. V podkapitolách 4.3.1 až 4.3.4 následovalo ověřování konkrétních finančních a makroekonomických indikátorů v dlouhém období. Byl potvrzen vztah mezi cenou Bitcoinu a hodnotou Dow Jones indexu. Nepotvrdila se předchozí koncepce závislosti mezi cenou Bitcoinu a hodnotou směnného kurzu USD/EUR, resp. cenou ropy. V kontrastu s předpoklady byla objevena nepřímá závislost mezi cenou Bitcoinu a cenou zlata. V samostatné podkapitole byl ověřen vliv všech těchto veličin na cenu Bitcoinu v krátkém období. Všechny výsledky byly patřičně ekonomicky interpretovány.

5 Závěr

Cílem této bakalářské práce bylo empiricky ověřit vliv finančních a makroekonomických ukazatelů na vývoj ceny Bitcoinu. Naplnění těchto cílů bylo dosaženo pomocí vědeckých metod syntézy a deskriptivní a korelační analýzy.

První ze tří částí této práce byla zaměřena na peníze obecně. Nejprve byl stručně popsán jejich historický vývoj. Nejstarším typem peněz byly tzv. komoditní peníze, které lidstvo začalo používat v souvislosti s rozvojem nepřímé směny. Jako nejvhodnější se osvědčilo používání drahých kovů, které díky svým vlastnostem vyhovovaly požadavkům obecně přijímaného platebního prostředku. Později se začaly razit plnohodnotné peníze – mince, jejichž kupní síla odpovídala váhovému množství drahého kovu v nich obsaženém a nákladů na jejich ražbu. Jako první bankovky pak sloužily původně stvrzenky o množství drahého kovu uloženého u zlatníka (resp. v bance). To byl počátek neplnohodnotných peněz. Dále byly peníze definovány z teoretického a z empirického hlediska. Teoreticky byly peníze definovány jako vše, co je všeobecně přijímáno při placení zboží a služby nebo při úhradě dluhu. Empiricky byly peníze definovány pomocí peněžních agregátů, které jsou sestavovány centrálními bankami. Následovalo vysvětlení funkcí peněz. Těmi jsou zpravidla funkce prostředku směny, funkce účetní jednotky a funkce uchovatele hodnoty. V další kapitole bylo vysvětleno, co je to měna. Jde o národní, resp. nadnárodní formu peněz (v případě měn jako je Euro). Každou měnu charakterizují její technické a ekonomické znaky. V závěru této části práce byl pomocí postkeynesiánské teorie endogenních peněz objasněn vznik a zánik peněz. Nejvíce peněz v bankovním systému vzniká, když obchodní banky poskytují úvěry nebankovním jednotkám. Naopak nejvíce peněz zaniká splácením úvěrů včetně úroků bankám. Podle teorie endogenních peněz úvěry vytvářejí vklady, není proto nutné aby při poskytování úvěrů nejdříve někdo peníze do banky přinesl. Dochází-li k poskytování podvodných úvěrů, hovoří se o tzv. tunelování.

Druhá část práce byla zaměřena již na samotný Bitcoin. Byly zde uvedeny 2 různá hlediska na definici Bitcoinu – Bitcoin jako platební systém a Bitcoin jako digitální měna. Bitcoin jako platební systém vyniká především svojí nezávislostí na jakékoli centrální autoritě a umožňuje kterýmkoliv dvěma stranám uskutečňovat transakce přímo mezi sebou. Bitcoin je také typem digitální měny, která používá kryptografii (šifrování) k zabezpečování transakcí a k řízení emise nových jednotek. Do kategorie digitálních měn spadají také virtuální měny, od nich se však Bitcoin výrazně liší aspektem centralizace. Potom následovala kapitola zaměřená na identitu autora Bitcoinu, Satoshiho Nakamota. O její odhalení se již pokoušelo velké

množství lidí, avšak pokaždé neúspěšně. Existují i domněnky, že jde o pseudonym, za kterým se neskrývá jen jeden člověk, ale celá skupina lidí. Poslední dvě kapitoly této části měly spíše techničtější charakter a obsahovaly popis základních mechanismů a principů těžby bitcoinů, resp. procesu provádění transakcí. Základním prvkem v procesu těžby bitcoinů jsou „těžaři“, kteří mezi sebou navzájem soutěží. Jejich úkolem je najít náhodně vygenerovaný řetězec dat zvaný nonce, který společně s hashem předchozího bloku a hashem transakcí vytvoří výsledný hash splňující podmínky stanovené Bitcoinem. Hash je produktem algoritmu, který dokáže transformovat různě velké objemy dat na stejně velké zdánlivě náhodné sekvence písmen a číslic. Těžaři, kterému se povede vytvořit vyhovující výsledný hash, náleží odměna ve výši 25 bitcoinů plus suma poplatků přiložených k jednotlivým transakcím v daném bloku. Transakce bitcoinů fungují na zcela unikátním principu, který umožňuje, že samotné bitcoiny nemusí být nikde uložené. Důležité jsou tzv. neutracené výstupy transakcí, které v block chainu „čekají“, dokud je „neutratí“ vstup nějaké jiné transakce. Jsou-li hodnoty výstupu a vstupu transakce nekompatibilní, jsou vytvořeny dva výstupy, z nichž jeden představuje „vrácení drobných“ plátci transakce.

Ve třetí části této práce byla na konkrétních datech ověřena platnost teoretických i empirických poznatků uvedených v dostupné literatuře. Důvodem pro ověřování byla skutečnost, že většina autorů prováděla svoji analýzu před téměř dvěma roky, což v případě Bitcoinu představuje dávnou minulost. Ověřování bylo provedeno pomocí korelační analýzy, která spočívala ve výpočtu Pearsonova koeficientu korelace a následné interpretaci výsledků. Byly zde také identifikovány hlavní faktory působící na vývoj ceny Bitcoinu. Patří mezi ně nabídka, která je v případě Bitcoinu pevně stanovená, a poptávka, na níž působí další vlivy. Mezi vedlejší faktory patří např. nedostatečná akceptace Bitcoinu ekonomickými subjekty či vliv médií. Byl učiněn závěr, že největší vliv na vývoj ceny Bitcoinu mají výkyvy v poptávce po Bitcoinu. Vliv konkrétních finančních a makroekonomických indikátorů na cenu Bitcoinu byl nejprve ověřen v dlouhém období, které vzniklo prodloužením původního období použitého v jiné předchozí práci. V tomto období byl potvrzen vztah mezi cenou Bitcoinu a hodnotou Dow Jones indexu. Nepotvrdila se předchozí koncepce závislosti mezi cenou Bitcoinu a hodnotou směnného kurzu USD/EUR, resp. cenou ropy. V tomto období byla rovněž v kontrastu s předpoklady objevena nepřímá závislost mezi cenou Bitcoinu a cenou zlata. Na výsledcích za krátké období (2. 12. 2013 – 27. 3. 2015) se výrazně podepsal klesající trend ceny Bitcoinu následující po obrovském cenovém nárůstu, který Bitcoin zaznamenal ke konci roku 2013. Příliš vysoká cena neodrážela skutečný stav nabídky a poptávky a ukázala se jako dlouhodobě neudržitelná. Výsledky korelační analýzy tak nevyšly podle očekávání, což

zapříčinilo obtížnou interpretaci v některých případech. Důvodem mohly být také nesprávně stanovené předpoklady uvedené v kapitole 4.3.

Samotná metoda korelační analýzy se v některých ohledech ukázala jako nedostatečná. Mezi výhody této metody patří relativně snadná proveditelnost, jednou z nevýhod je však nižší vypovídací hodnota výsledků. Především v dlouhém období, kdy se cena Bitcoinu po většinu času téměř nevyvíjela, dochází kvůli tomu, jak je Pearsonův korelační koeficient koncipován, k velkému zkreslování výsledků. Autor práce proto doporučuje v budoucích výzkumech v této oblasti použití pokročilejších a komplexnějších metod.

Pro účely této práce a kvůli omezenému času na výzkum bylo učiněno rozhodnutí z větší části se spolehnout na již v minulosti testované ukazatele. Avšak většina vybraných indikátorů byla určitým způsobem spjata s hospodářstvím Spojených států, což se v současné době může jevit jako nesprávná volba. Přibližně 50% objemu veškerých nákupů a prodejů bitcoinů probíhá na největší čínské burze BTCChina (viz Bitcoincharts, 2015) obchodující výhradně v čínských jüanech. Případný budoucí výzkum vedený podobnými metodami by proto měl zahrnovat i ukazatele spojené s čínskou ekonomikou.

Hlavním pozorovaným jevem v této bakalářské práci byla cena Bitcoinu nikoliv hodnota Bitcoinu. Budoucí výzkum by proto mohl být zaměřen na hledání odpovědi na otázku, jak velký podíl má na hodnotě Bitcoinu to, na kolik si jej lidé cení jako prostředku směny, nebo do jaké míry ji tvoří náklady na jeho těžbu.

Seznam použité literatury

BANK OF ENGLAND. Innovations in payment technologies and the emergence of digital currencies. *Quarterly Bulletin 2014 Q3* [online]. 2014, Vol. 54, No. 3 [cit. 23. 2. 2015]. ISSN 0005-5166. Dostupné z: http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q301.pdf

BITCOINCHARTS. Exchange volume distribution [online]. Lübeck: bitcoincharts.com, 30. 4. 2015 [cit. 30. 4. 2015]. Dostupné z: http://bitcoincharts.com/charts/volumepie/

BITCOIN.ORG. *Frequently Asked Questions* [online]. Washington, D.C.: Bitcoin Foundation, 2015a, [cit. 27. 2. 2015]. Dostupné z: https://bitcoin.org/en/faq

BITCOIN.ORG. *Bitcoin Developer Guide* [online]. Washington, D.C.: Bitcoin Foundation, 2015b, [cit. 15. 3. 2015]. Dostupné z: https://bitcoin.org/en/developer-guide

BLOCKCHAIN. *View information about a bitcoin transaction* [online]. New York: Blockchain.info, 2015a [cit. 23. 2. 2015]. Dostupné z: https://blockchain.info/tx/426cd3fa4e2cad2226395f8a033d78315f1fdca1df52d1bdad305ac73cff5db8

BLOCKCHAIN. *Blockchain size* [online]. New York: Blockchain.info, 2015b [cit. 19. 3. 2015]. Dostupné z: https://blockchain.info/charts/blocks-size

BLOCKCHAIN. *Total Bitcoins in Circulation* [online]. New York: Blockchain.info, 2015c [cit. 29. 3. 2015]. Dostupné z: https://blockchain.info/charts/total-bitcoins

BLOCKCHAIN. *Market Price (USD)* [online]. New York: Blockchain.info, 2015d [cit. 24. 4. 2015]. Dostupné z: https://blockchain.info/charts/market-price

BLOCKCHAIN. *Number of Transactions Excluding Chains Longer Than 10* [online]. New York: Blockchain.info, 2015e [cit. 24. 4. 2015]. Dostupné z: https://blockchain.info/charts/n-transactions-excluding-chains-longer-than-10

BUCHHOLZ, M., DELANEY, J., WARREN, J. and J. Parker. Bits and Bets, Information, Price Volatility, and Demand for BitCoin. *Economics 312*, 2012. Dostupné z: http://www.bitcointrading.com/pdf/bitsandbets.pdf

CIAIAN, P., M. RAJČÁNIOVÁ a d'Artis KANCS. The Economics of BitCoin Price Formation. In *EERI Research Paper Series.* 2014, No. 8, pp. 2-22. ISSN 2031-4892.

COINDESK. *How to Set Up a Bitcoin Miner* [online]. Londýn: CoinDesk.com, 26. 11. 2013, [cit. 15. 3. 2015]. Dostupné z: http://www.coindesk.com/information/how-to-set-up-a-miner/

COINDESK. *What is Bitcoin?* [online]. Londýn: CoinDesk.com, 20. 2. 2014a, [cit. 27. 2. 2015]. Dostupné z: http://www.coindesk.com/information/what-is-bitcoin/

COINDESK. *How to Store Your Bitcoins* [online]. Londýn: CoinDesk.com, 22. 12. 2014b, [cit. 28. 2. 2015]. Dostupné z: http://www.coindesk.com/information/how-to-store-your-bitcoins/

COINDESK. *How do Bitcoin Transactions Work?* [online]. Londýn: CoinDesk.com, 6. 3. 2014c, [cit. 13. 3. 2015]. Dostupné z: http://www.coindesk.com/information/how-do-bitcoin-transactions-work/

COINDESK. *How Bitcoin Mining Works?* [online]. Londýn: CoinDesk.com, 22. 12. 2014d, [cit. 13. 3. 2015]. Dostupné z: http://www.coindesk.com/information/how-bitcoin-mining-works/

COINDESK. *Who is Satoshi Nakamoto?* [online]. Londýn: CoinDesk.com, 2. 1. 2015, [cit. 7. 3. 2015]. Dostupné z: http://www.coindesk.com/information/who-is-satoshi-nakamoto/

ČERNOHORSKÝ, Jan a Petr TEPLÝ. *Základy financí.* Praha: Grada Publishing, 2011. ISBN 978-80-247-3669-3.

ČESKÁ NÁRODNÍ BANKA. *Bankovní rada ČNB* [online]. Praha: ČNB, 2015 [cit. 16. 2. 2015]. Dostupné z: https://www.cnb.cz/cs/o_cnb/bankovni_rada/

ČESKÁ NÁRODNÍ BANKA. *Harmonizované peněžní agregáty České republiky* [online]. Praha: ČNB, 2014 [cit. 11. 12. 2014]. Dostupné z: http://www.cnb.cz/cs/statistika/menova_bankovni_stat/stat_mb_met/stat_mb_harmon_agregaty.html

DAVIS, Joshua. The Crypto-Currency. *The New Yorker* [online]. October 10, 2011 Issue [cit. 22. 2. 2015]. ISSN 0028-7369. Dostupné z: http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency

EVROPSKÁ CENTRÁLNÍ BANKA. *Virtual Currency Schemes* [online]. Frankfurt am Main: ECB, October 2012 [cit. 21. 2. 2015]. Dostupné z: http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

ELLIOT, Francis and Gary DUNCAN. Chancellor Alistair Darling on brink of second bailout for banks. *The Times* [online]. Londýn: Times Newspapers, 3. 1. 2009 [cit. 6. 3. 2015]. Dostupné z: http://www.thetimes.co.uk/tto/business/industries/banking/article2160028.ece

GOODMANOVÁ, Leah McGrath. The Face Behind Bitcoin. *Newsweek* [online]. Londýn: Newsweek, 6. 3. 2014 [cit. 8. 3. 2015]. Dostupné z: http://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html

GORALE, Alex, Fake Transaction Chains Double 2014 Bitcoin Volume. *Cryptocoins News* [online]. Oslo: PF Wetting, 3. 1. 2015 [cit. 4. 4. 2015]. Dostupné z: https://www.cryptocoinsnews.com/fake-transaction-chains-double-2014-bitcoin-volume/

GREENBERG, Andy. FBI Says It's Seized $28.5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road. *Forbes* [online]. Jersey City: Forbes Media, 25. 10. 2013 [cit. 24. 4. 2015]. Dostupné z: http://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/

JANSSEN, Cory. Peer-To-Peer Network (P2P Network). *Techopedia* [online]. Edmonton: Janalta Interactive, 2015a [cit. 23. 2. 2015]. Dostupné z: http://www.techopedia.com/definition/25777/peer-to-peer-network-p2p-network¨

JANSSEN, Cory. Massively Multiplayer Online Game (MMOG). *Techopedia* [online]. Edmonton: Janalta Interactive, 2015b [cit. 21. 2. 2015]. Dostupné z: http://www.techopedia.com/definition/27054/massively-multiplayer-online-game-mmog

JÍLEK, Josef. *Peníze a měnová politika*. Praha: Grada Publishing, 2004. ISBN 80-247-0769-1.

JÍLEK, Josef. *Finance v globální ekonomice I. Peníze a platební styk.* Praha: Grada Publishing, 2013. ISBN 978-80-247-3893-2.

JUREČKA, Václav a kol. *Mikroekonomie.* Praha: Grada Publishing, 2010. ISBN 978-80-247-3259-6.

KING, N., V. OKSMAN and Ch. BRY. *Updating and distributing encryption keys.* Spojené Státy Americké. US 20100042841 A1, Zdrojový dokument #12192809. 2008-08-15. Dostupné z: http://www.freshpatents.com/-dt20100218ptan20100042841.php

KRISTOUFEK, Ladislav. BitCoin meets Google Trends and Wikipedia: Quantifying the relationship between phenomena of the Internet era. *Scientific Reports 3* (3415), 2013. Dostupné z: http://www.nature.com/srep/2013/131204/srep03415/pdf/srep03415.pdf

METCALF, Allan. The Latest Style. *The Chronicle of Higher Education* [online]. Washington, D. C.: The Chronicle of Higher Education, 11. 4. 2014 [cit. 20. 2. 2015]. Dostupné z: http://chronicle.com/blogs/linguafranca/2014/04/11/the-latest-style/

MISHKIN, Frederic S. *The economics of money, banking, and financial markets.* 7. vyd. Upper Saddle River: Prentice Hall, 2004. ISBN 0-321-12235-6.

NAKAMOTO, Satoshi. *Bitcoin P2P e-cash paper* [online]. Kalifornie: The Mail Archive, 1. 11. 2008 [cit. 6. 3. 2015]. Dostupné z: http://www.mail-archive.com/cryptography%40metzdowd.com/msg09959.html

NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System* [online]. Palo Alto: bitcoin.org, 24. 3. 2009 [cit. 22. 2. 2015]. Dostupné z: https://bitcoin.org/bitcoin.pdf

PALMER, Daniel. Dorian Nakamoto Hires Lawyer, Denies Knowledge of Bitcoin. *CoinDesk* [online]. Londýn: CoinDesk.com, 17. 3. 2014, [cit. 8. 3. 2015]. Dostupné z: http://www.coindesk.com/dorian-nakamoto-hires-lawyer-denies-knowledge-bitcoin/

PENENBERG, Adam L. The Bitcoin Crypto-Curreny Mystery Reopened. *Fast Company* [online]. New York: Fast Company Magazine, 11. 11. 2011 [cit. 7. 3. 2015]. Dostupné z: http://www.fastcompany.com/1785445/bitcoin-crypto-currency-mystery-reopened

QUANDL.COM. *Find and Use Data. Easily.* [online] Toronto: Quandl, 2015. Dostupné z: https://www.quandl.com/

REVENDA, Zbyněk. Monopoly centrálních bank a emise peněz. *Politická ekonomie*, Vol. 57, no. 5, 2009.

REVENDA, Zbyněk. *Peníze a zlato.* 2. vyd. Praha: Management Press, 2013. ISBN 978-80-7261-260-4.

RIEGEL, Karel. *Ekonomická psychologie.* Praha: Grada Publishing, 2007. ISBN 978-80-247-1185-0.

ŠÍMA, Josef. Deflace – definiční znak zdravé ekonomiky. *Finance a úvěr*, 52. vydání. 2002, číslo 10, str. 539-549. Dostupné z: http://journal.fsv.cuni.cz/storage/683_539_549.pdf

URQUHART, Jim. 'China's Google' begins accepting Bitcoin. *RT: Question More.* [online]. London: Autonomous Nonprofit Organization "TV-Novosti", 16. 10. 2013, aktualizováno 17. 10. 2013, [cit. 26. 4. 2015]. Dostupné z: http://rt.com/news/china-baidu-accept-bitcoin-276/

VAN WIJK, Dennis. *What can be expected from the BitCoin?* Working Paper No. 345986, Erasmus Rotterdam Universiteit, 2013. Dostupné z: http://thesis.eur.nl/pub/14100/Final-version-Thesis-Dennis-van-Wijk.pdf

VAROUFAKIS, Yanis. *It all began with a strange email* [online]. Bellevue: Valve Corporation, 14. 6. 2012 [cit. 21. 2. 2015]. Dostupné z: http://blogs.valvesoftware.com/economics/it-all-began-with-a-strange-email/

VAROUFAKIS, Yanis. Bitcoin and the dangerous fantasy of 'apolitical' money. *Yanis Varoufakis: Thoughts for the Post-2008 World* [online]. WordPress.com, 22. 4. 2013 [cit. 29. 3. 2015]. Dostupné z: http://yanisvaroufakis.eu/2013/04/22/bitcoin-and-the-dangerous-fantasy-of-apolitical-money/

VIGNA, Paul and Michael J. CASEY. BitBeat: Is It Bitcoin, or bitcoin? The Orthography of the Cryptography. *The Wall Street Journal* [online]. New York: Dow Jones & Company, 14. 3. 2014 [cit. 20. 2. 2015]. Dostupné z: http://blogs.wsj.com/moneybeat/2014/03/14/bitbeat-is-it-bitcoin-or-bitcoin-the-orthography-of-the-cryptography/

WAGNER, Andrew. Digital vs. Virtual Currencies. *Bitcoin Magazine* [online]. Issue 22, Huntsville: BTC Media, 22. 8. 2014 [cit. 20. 2. 2015]. Dostupné z: https://bitcoinmagazine.com/15862/digital-vs-virtual-currencies/

WALLACE, Benjamin. The Rise and Fall of Bitcoin. *Wired* [online]. New York: Wired, 23. 11. 2011 [cit. 6. 3. 2015]. Dostupné z: http://www.wired.com/2011/11/mf_bitcoin/all/

Zákon č. 6 ze dne 17. prosince 1992 o České národní bance. In: *Sbírka zákonů České republiky*. 1993, částka 3, s. 36. Dostupný také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=22435

Seznam zkratek

ASIC	Application Specific Integrated Circuit
ČNB	Česká národní banka
EU	Evropská unie
Fed	Federální systém rezerv
FBI	Federal Bureau of Investigation
GB	Gigabyte
MB	Megabyte
MMO	Massive Multiplayer Online
NASDAQ	National Association of Securities Dealers Automated Quotations
NOW	Negotiable Order of Withdrawal
NYSE	New York Stock Exchange
P2P	Peer-to-peer
UTXO	Unspend Transaction Output
WTI	West Texas Intermediate

Prohlašuji, že

- jsem byl seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, bakalářskou práci užít (§ 35 odst. 3);
- souhlasím s tím, že bakalářská práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího bakalářské práce. Souhlasím s tím, že bibliografické údaje o bakalářské práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, bakalářskou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Karviné dne 27.4.2015

Jiří Chadýra
.....
jméno a příjmení studenta